FD-302 (Rev. 5-8-10)

FEDERAL BUREAU OF INVESTIGATION

Date of entry 06/07/2021

On June 7, 2021, writer downloaded a class action lawsuit filed against SolarWinds Corporation. The lawsuit names [redacted] as a former SolarWinds employee who warned SolarWinds' executives of SolarWinds' cyber security problems.

b6
b7C

The lawsuit will be kept in the 1A sub-file.

Investigation on 06/07/2021 at San Antonio, Texas, United States (, Other (PACER Download))

File # 318D-SA-3360310 Date drafted 06/07/2021

by [redacted]

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

FILED
2021 JUN -1 PM 1:06
CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY

IN RE SOLARWINDS CORPORATION SECURITIES LITIGATION

Case No. 1:21-cv-00138-RP

CLASS ACTION

JURY TRIAL DEMANDED

CONSOLIDATED COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS

TABLE OF CONTENTS

Page(s)

I. INTRODUCTION 1

II. JURISDICTION AND VENUE 6

III. THE PARTIES 7

A. Lead Plaintiff 7

B. The Corporate Defendant 7

C. The Executive Defendants 7

D. The Controlling Entity Defendants 8

IV. SUMMARY OF THE FRAUD 9

A. Background 9

1. The Private Equity Firms Invest in SolarWinds 9

2. SolarWinds' Software Gains Widespread Use in the Federal Government and Beyond 11

3. SolarWinds Assures Customers and Investors That It Adheres to Its "Security Statement" 14

B. Unknown to Investors at the Time, SolarWinds' Internal Security Was in Shambles and the Company Did Not Adhere To Its Security Statement 27

1. SolarWinds Executives Were Told About the Company's Deficient Cybersecurity Controls 27

2. SolarWinds Refuses to Reform, Causing Its Global Cybersecurity Strategist to Resign in Protest 34

3. SolarWinds Is Told That the Password To Access Its Internal Update Server Was Publicly Available On the Internet For Years 41

4. SolarWinds Lacked the Cybersecurity Protections That It Represented in Its Security Statement 45

C. Customers and Investors Learn That SolarWinds Fails To Maintain Cybersecurity 58

D. SolarWinds Is Forced To Admit It Lacked Sufficient Security Measures During the Class Period 65

E. The SEC, Department of Justice, State Attorneys General Launch Investigations Into SolarWinds, But the Company Still Pays Its Executives Lavishly 68

V. ADDITIONAL ALLEGATIONS OF SCIENTER 69

VI. DEFENDANTS' MATERIALLY FALSE AND MISLEADING STATEMENTS AND OMISSIONS 78

A. Defendants' Materially False and Misleading Statements and Omissions in Their "Security Statement" 78

B. Defendants' Additional Materially False and Misleading Statements and Omissions on the SolarWinds Website 82

C. Defendants' Additional Materially False and Misleading Statements and Omissions Throughout the Class Period 84

1. March 14, 2019 Interview 84

2. April 30, 2019 Interview 85

VII. LOSS CAUSATION 86

VIII. INAPPLICABILITY OF THE STATUTORY SAFE HARBOR 90

IX. PRESUMPTION OF RELIANCE 91

X. CLASS ACTION ALLEGATIONS 92

XI. CLAIMS FOR RELIEF 93

COUNT I VIOLATIONS OF SECTION 10(B) OF THE EXCHANGE ACT AND RULE 10b-5 PROMULGATED THEREUNDER (Against SolarWinds and the Executive Defendants) 93

COUNT II VIOLATIONS OF SECTION 20(A) OF THE EXCHANGE ACT (Against the Control Person Defendants) 96

XII. PRAYER FOR RELIEF 99

XIII. JURY DEMAND 99

Lead Plaintiff New York City District Council of Carpenters Pension Fund ("Lead Plaintiff"), by and through its counsel, brings this action under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act") on behalf of itself and all persons and entities, except Defendants and their affiliates, who purchased or otherwise acquired the securities of SolarWinds Corporation. ("SolarWinds" or the "Company") between October 18, 2018 and December 17, 2020, inclusive (the "Class Period") and were damaged thereby.

I. INTRODUCTION

1. SolarWinds sells network monitoring software to a significant portion of the United States federal government and the majority of Fortune 500 companies in the United States. Its customers include the U.S. Pentagon, State Department, the Office of the President of the United States, the FBI, the Secret Service, and the National Nuclear Security Administration—customers whose data is among the most sensitive in the world.

2. Throughout the Class Period, the Company falsely and misleadingly told investors that it had a robust cybersecurity program and adhered to specific cybersecurity practices set forth in a "Security Statement" prominently featured on its website. In reality, the Company—which was primarily owned and controlled by two private equity firms, Silver Lake Partners, LLC and Thoma Bravo, LP—sacrificed cybersecurity to generate short-term profits for its principal owners. The truth was gradually revealed beginning on December 13, 2020, when it was reported that the Company's software was the source of the largest cyberattack in U.S. history. A series of revelations regarding the Company's deficient cybersecurity practices ensued, and investors learned that the Company, contrary to its years of assurances to investors, failed to adhere to the cybersecurity practices that it told them it followed.

3. Throughout the Class Period, SolarWinds and its top executives sought to leverage customer concerns by touting their commitment to cybersecurity and expertise in the cybersecurity

space. The Company showcased its "Security Resource Center" on its website, which compiled information about cybersecurity trends and recommended best practices to keep its customers safe from cyberattacks. The Company assured customers and investors that it was not only committed to cybersecurity but also followed specific practices to ensure the security of its products—and, by extension, customers' data. Featured prominently in its Security Resource Center, and accessible from any page on the website, was the Company's Security Statement, which contained a series of representations regarding the Company's cybersecurity. In the Security Statement, the Company represented that it followed a host of particular cybersecurity practices, including having a "Security Team," an "Information Security Policy," providing "security training" to its employees, following a "Password Policy," limiting "user authorization," keeping its network "segmented," and adhering to the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework, including performing background checks on employees. Experts have recognized the basic—and critical—nature of each of these practices.

4. SolarWinds and its executives bolstered these representations with additional assurances that the Company prioritized cybersecurity. The Company's chief security spokesman—Defendant Tim Brown—spoke frequently about the Company's supposed cybersecurity. Over and over, he stated that the Company "focused on ... heavy-duty hygiene," and that SolarWinds "places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards." These tactics helped the Company build up its customer base during the Class Period, as it gained 300,000 customers worldwide and more than $230 million in federal government contracts.

5. The Company's assurances regarding its cybersecurity were also important to investors. The Company's representations enabled it to complete two public offerings, selling

over $375 million in Company stock at the start of the Class Period and another $270 million just months later. The Defendants also profited personally during the Class Period from their private sales of the Company's stock, which increased in price by over 50% during the Class Period.

6. Unknown to investors at the time, the Company knew prior to the Class Period that its internal cybersecurity practices were woefully deficient and not as represented. Lead Counsel spoke with Ian Thornton-Trump, SolarWinds' former Global Cybersecurity Strategist. Mr. Thornton-Trump explained to Lead Counsel that the Company failed to follow a host of basic cybersecurity practices. For instance, Mr. Thornton-Trump described how, during his time at SolarWinds, there was no security team, there was no password policy, there was no documentation regarding data protection and controls, and the Company did not limit user access controls, exposing the Company's "crown jewels" to a potential cyberattack. He stated that, "from a security perspective, SolarWinds was an incredibly easy target to hack." Mr. Thornton-Trump's concerns led him, in April 2017, to convene several of the Company's top executives and give a presentation on the Company's deficient cybersecurity practices. During his presentation, Mr. Thornton-Trump stressed that changes were necessary, warning that "[t]he survival of our customers depends on a commitment to build secure solutions" and "[t]he survival of the company depends on an internal commitment to security." The Company refused to implement the changes in Mr. Thornton-Trump's presentation because the Company's then-CEO, Kevin Thompson, did not want to spend the money to do so. Mr. Thornton-Trump resigned in protest.

7. The Company's deficient cybersecurity practices exposed the Company to cyberattack throughout the Class Period. On November 11, 2019, a cybersecurity researcher notified the Company in writing that the password to its Update Server—the server from which customers downloaded software updates for the Company's products—had been publicly available

on the internet for approximately one-and-a-half years. On June 17, 2018, a SolarWinds employee—later identified by the Company as an intern—had posted the password along with credentials and a link to the Update Server on a public website. In addition to being publicly available, the password to access the Update Server was "solarwinds123"—an almost comically easy-to-guess and insecure password. The researcher that identified the compromised password warned the Company at the time that "any hacker could [have] upload[ed] malicious [files]" to the Update Server using the publicly-available credentials and password.

8. SolarWinds never disclosed any of these facts. Nor did it disclose that, contrary to its assurances to investors, it never followed the cybersecurity practices it purported to. In addition to Mr. Thornton-Trump, a host of former SolarWinds employees have explained that the Company lacked the cybersecurity protections it claimed to have in its "Security Statement." *First*, the Company had no "security team." Former employees of the Company repeatedly report never having heard of or interacted with any such team at the Company, with one former employee stating, "If there was one, they had a really plush job because they didn't do anything." *Second*, the Company had no "security information policy." Former employees never saw or heard of such a policy, even though Mr. Thornton-Trump specifically asked his colleagues to see it. *Third*, the Company did not have or enforce a "password policy." Former employees recounted that they never received any policies, direction or training regarding secure passwords. They further explained that "solarwinds123"—the compromised, publicly available password—was commonly used at the Company, and other passwords were "hard-coded" and never changed for years. *Fourth*, the Company did not provide cybersecurity training to its employees. Several former employees explained that this training simply did not exist at SolarWinds, and that nobody at the Company spoke with them about maintaining good cybersecurity. *Fifth*, the Company neither

segmented its network nor limited user access to those parts of the SolarWinds network related to their job functions. As a result, SolarWinds employees had free-wheeling access to the Company's critical Update Server and other "crown jewels." *Sixth,* the Company did not even perform basic background checks on its employees, notwithstanding concerns raised by the Company's human resource department. *Finally*, the Company did not prioritize internal cybersecurity. Former employees have recounted how Defendant Thompson and the private equity firms that controlled SolarWinds sacrificed cybersecurity to boost short-term profits. As *The New York Times* reported, when Defendant Thompson became the CEO of the Company, "every part of the business was examined for cost savings and common security practices were eschewed because of their expense." Experts have tied the cyberattack directly to this cost-cutting strategy, concluding that "the same sloppy and corrupt practices that allowed [the] massive cybersecurity hack made [the CEO of the private equity firm that owns SolarWinds] a billionaire."

9. Investors first began to learn about the Company's deficient cybersecurity practices on December 13, 2020, when it was leaked to the press that cybercriminals had entered SolarWinds' systems and used its Update Server to execute the largest cyberattack in U.S. history. Cybercriminals—who had unfettered access to the Company's server for nearly two years prior to this disclosure—injected malicious code into a SolarWinds software update, which was then disseminated to tens-of-thousands of the Company's customers via the Update Server. After the revelation of the cyberattack, a full picture of the Company's deficient cybersecurity practices became public, including the fact that the Company had been warned of its deficient cybersecurity practices before and during the Class Period, that the Company failed to remove the malware from its Update Server even after learning that its software updates were being downloaded by

customers, and that the federal Cybersecurity and Infrastructure Security Agency ordered all federal agencies to cease using the Company's products due to the "unacceptable risks" posed.

10. Investors suffered immensely as a result of the Company's misrepresentations and omissions. As the truth was revealed over the course of several disclosures, the price of SolarWinds' stock cratered. All told, over the course of just a few days, the Company's share price plummeted 34%. Meanwhile, Defendants profited handsomely. From the beginning of the Class Period, Defendants reaped $730 million in proceeds from their sales of SolarWinds stock, including through the private equity firms' sale of over $450 million in their own stock, less than seven days before the initial disclosures that caused investors' substantial losses.

II. JURISDICTION AND VENUE

11. The claims alleged herein arise under Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)), and Rule 10b-5 promulgated thereunder (17 C.F.R. § 240.10b5). This Court has jurisdiction over the subject matter of this action pursuant to Section 27 of the Exchange Act (15 U.S.C. § 78aa) and 28 U.S.C. § 1331.

12. Venue is proper in this District pursuant to Section 27 of the Exchange Act (15 U.S.C. § 78aa) and 28 U.S.C. § 1391(b). SolarWinds maintains its headquarters in Austin, Texas, conducts substantial business in this District, and many of the acts and conduct that constitute the violations of law complained of herein, including dissemination to the public of materially false and misleading information, occurred in and were issued from this District. In connection with the acts alleged in this Complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the mails, interstate telephone communications, and the facilities of the national securities markets.

III. THE PARTIES

A. Lead Plaintiff

13. Lead Plaintiff New York City District Council of Carpenters Pension Fund provides retirement benefits to over 30,000 working and retired carpenters and their families. As set forth in the certification previously filed with the Court (ECF No. 1), Lead Plaintiff purchased SolarWinds common stock during the Class Period and suffered damages as a result of the violations of the federal securities laws alleged herein.

B. The Corporate Defendant

14. Defendant SolarWinds is a Delaware corporation with its executive offices located at 7171 Southwest Parkway, Building 400, Austin, Texas 78735. SolarWinds is majority-owned and controlled by two private equity firms, Silver Lake Partners, LLC and Thoma Bravo LP, which acquired SolarWinds in 2015, took the Company private in 2016, and then took the Company public again in October 2018, at the start of the Class Period. The Company's common stock trades on the New York Stock Exchange ("NYSE") under the ticker symbol "SWI." As of October 2020, there were over 314 million shares of SolarWinds common stock outstanding.

C. The Executive Defendants

15. Defendant Kevin B. Thompson ("Thompson") was SolarWinds' President and Chief Executive Officer ("CEO") until his resignation on December 31, 2020. SolarWinds announced Thompson's resignation on December 9, 2020, just four days before the revelations of the Company's deficient cybersecurity controls. Nevertheless, the Company paid Defendant Thompson $25.5 million in cash and incentive awards in 2020 alone. SolarWinds continues to pay Defendant Thompson in exchange for his cooperation in the defense of the Company against ongoing investigatory probes and legal challenges, including payments of $312,500 thus far.

16. Defendant Tim Brown ("Brown") has been SolarWinds' Vice President of Security Architecture since 2017. Brown claims decades of experience in the security technology field. During the Class Period, Brown was, in his own words, "responsible for the security of [SolarWinds'] products ... as well as security for [its] infrastructure."[1] Brown was one of SolarWinds' most public-facing executives during the Class Period, frequently appearing on podcasts and interviews touting the Company's supposed cybersecurity practices and policies.

17. Defendants Thompson and Brown are collectively referred to herein as the "Executive Defendants."

D. The Controlling Entity Defendants

18. SolarWinds was a "controlled company" during the Class Period and was specifically identified as such in its SEC filings. Two private equity firms—Defendants Silver Lake Partners, LLC ("Silver Lake") and Thoma Bravo, LP (f/k/a Thomas Bravo, LLC) ("Thoma Bravo")—owned over 80% of the Company's stock at the start of the Class Period and exercised control over SolarWinds throughout the Class Period.

19. Defendant Silver Lake is one of the two private equity firms that controlled SolarWinds during the Class Period. Silver Lake and its affiliate funds owned over 40% of the Company's stock at the start of the Class Period. In addition, its Managing Partner and Managing Director (Kenneth Y. Hao and Mike Bingle, respectively) and two of its Directors (Jason White and Mike Widmann) sat on SolarWinds' Board of Directors while simultaneously being employed by Silver Lake. Silver Lake sold $135 million worth of SolarWinds shares in a May 2019 follow-

[1] *Disruptive*, "Interview – Tim Brown – Solarwinds" available at: https://disruptive.live/story/tim-brown-interview-solarwinds/.

on offering, and $203 million of SolarWinds shares on December 7, 2020—less than a week before the revelations of the Company's deficient cybersecurity practices.

20. Defendant Thoma Bravo also controlled SolarWinds during the Class Period. Thoma Bravo, a private equity firm, and its affiliate funds owned over 40% of the Company's stock at the start of the Class Period. In addition, its Senior Operating Partner (James Lines), Managing Partner (Seth Boro), and Principal (Mike Hoffman) all sat on SolarWinds' Board of Directors while employed by Thoma Bravo. Thoma Bravo sold $135 million worth of SolarWinds shares in a May 2019 follow-on offering, and $256 million of its SolarWinds shares on December 7, 2020—less than a week before the revelations of the Company's deficient cybersecurity practices.

21. Throughout the Class Period, the majority of SolarWinds directors were representatives of either Thoma Bravo or Silver Lake. Defendants Silver Lake and Thoma Bravo are collectively referred to herein as the "Private Equity Firms" or "Controlling Entity Defendants."

22. The Executive Defendants and the Controlling Entity Defendants are collectively referred to herein as the "Control Person Defendants."

IV. SUMMARY OF THE FRAUD

A. Background

1. The Private Equity Firms Invest in SolarWinds

23. Between 2009 and 2015, SolarWinds was a publicly traded company. In early 2016, the Private Equity Firms purchased all of SolarWinds' public shares and took the Company private. The Private Equity Firms are known for identifying short-term profit-centers in software companies and leveraging them to sell all or part of their investment at a profit. As the *Wall Street Journal* explained, Thoma Bravo's business model consists of "identif[ying] software companies

with a loyal customer base but middling profits and transform[ing] them into moneymaking engines by retooling pricing, shutting down unprofitable business lines and adding employees in cheaper labor markets."[2] The Private Equity Firms executed this strategy with SolarWinds.

24. At the start of the Class Period, on October 19, 2018, the Private Equity Firms took SolarWinds public for the second time. This "take-private, then public" maneuver was familiar to the Private Equity Firms. Silver Lake took computer-chip manufacturer Smart Modular Technologies private in 2011 only to conduct a public offering a few years later, raising almost $60 million in the process. Likewise, just four years after acquiring a majority stake in the identity-management software company SailPoint Technologies, Thoma Bravo conducted a public offering in November 2018. In each instance, Silver Lake and Thoma Bravo respectively retained majority ownership of the companies after their public offerings.

25. The Private Equity Firms' "take-private, then public" multi-step strategy consists of (i) identifying an undervalued company with revenue growth opportunities, buying the company and taking the company private, oftentimes loading the company with debt in the meantime; (ii) cutting costs and growing revenues; and (iii) taking the streamlined company public again. In the process, the Private Equity Firms gradually sell their stock while still retaining as much control over the company as possible.

26. Experts have recently analyzed the Private Equity Firms' strategy, including their focus on short term-profits. As Rupert Carlyon, a financial executive and long-time investment banker, observed in discussing Defendant Silver Lake, "[t]he exit is going to be the primary return for them .... Fundamentally these funds are not set up to be long-term holders of capital."

---

[2] *Wall Street Journal,* "Orlando Bravo Rides Software Deals to Heights of Private-Equity Industry," (Sept. 22, 2020), available at: https://www.wsj.com/articles/orlando-bravo-rides-software-deals-to-heights-of-private-equity-industry-11600767001.

27. In purchasing SolarWinds and then taking it public again, then, the Private Equity Firms saw an opportunity to implement their strategy. In February 2016, the Private Equity Firms bought SolarWinds for $4.5 billion in cash and debt—each paying $1.3 billion in cash, and adding a total of $2 billion in debt—and took the Company private. The Private Equity Firms then privately applied their formula: they prioritized short-term revenue growth and aggressively cut costs outside of the public shareholders' view. Then, in 2018, the Private Equity Firms brought the new SolarWinds public again.

28. Once SolarWinds shares became publicly traded again at the start of the Class Period, the Private Equity Firms could more easily unload their shares to investors and satisfy their debt obligations. The IPO raised $375 million, and the Private Equity Firms netted an additional $260 million in a May 2019 follow-on offering. While unloading substantial amounts of shares for large profits, the Private Equity Firms maintained control over the Company's operations through their continued majority positions on the Company's Board of Directors. This control over the Company gave the Private Equity Firms the power to secretly prioritize their own short-term interests, while using shareholder funds to pay for it.

2. SolarWinds' Software Gains Widespread Use in the Federal Government and Beyond

29. Both before and during the Class Period, SolarWinds courted federal government agencies as customers. It offered government agencies software that enabled them to manage their networks, systems, and information technology infrastructure. The government contracting business was lucrative, with over $430 billion—almost 40% of all the federal government's total discretionary spending—directed towards contracts for services and goods per year.

30. To gain prominence in the software market for government agencies, SolarWinds needed to convince them that cybersecurity was a priority for the Company. Government agencies

require security and expect its vendors to do the same. The government thus relied on vendors' representations about their cybersecurity controls and best practices. During a keynote address on cybersecurity at the 2021 RSA Conference on Cybersecurity, Anne Neuberger—the Deputy National Security Advisor for Cyber and Emerging Technology—explained why representations regarding cybersecurity from vendors, such as SolarWinds, are so important. As she explained, "the government, and indeed all consumers, don't have visibility into what software is developed securely, and what's not.... Visibility engenders trust. And today we put our trust in vendors, but we do it blindly for the most part, because we don't have a way to measure that trust." Indeed, the Department of Defense requires prospective government contractors to follow the cybersecurity requirements set forth by the NIST, but relies on the vendors themselves to certify that the NIST requirements are, in fact, followed.

31. To gain the trust of government customers, SolarWinds emphasized that the Company was focused on cybersecurity and followed the NIST cybersecurity requirements. In touting its capabilities in its "SolarWinds Government White Paper: The Ultimate Guide To Federal IT Compliance," SolarWinds stressed that it "can help federal agencies with ... basic cyber hygiene," assuring federal agencies that "SolarWinds has the tools, expertise, and experience-based knowledge of the federal space to help any agency enhance its security posture, reduce risk, and more effectively protect agency data."

32. SolarWinds sought to exploit government agencies' and other prospective customers' concerns about cybersecurity by highlighting its capabilities and the severity and frequency of cyberattacks. To that end, on May 22, 2018, shortly before the Class Period, the Company issued a press release announcing the launch of its "Security Resource Center—a one-stop shop for the latest security news and resources." The stated purpose of its "Security Resource

Center" was to provide prospective customers "the information they need about current security issues and trends, as well as recommended best practices to help ensure their business and customers are protected." The Company highlighted that its "Security Resource Center will provide real-time alerts and important information from the field, including 'How-to Guides.'" The Company also highlighted how it would begin issuing "The Brown Report," a regular report authored by Defendant Brown, "which looks at the latest cybersecurity threats that may impact [managed service providers], and tackles each topic with an eye toward actions [managed service providers] can take today to help stay ahead of threats and help keep their clients safe from cyberattacks." The press release quoted Defendant Brown, who urged prospective customers to visit the Company's "Security Resource Center," which was located on its website and included the Company's "Security Statement."

33. Defendant Thompson also stressed to investors and prospective customers the cybersecurity threat landscape, and SolarWinds' purported role in protecting its customers. For example, during an investor conference, Defendant Thompson stated that "the threat landscape is getting worse, not better. My CIO likes to depress me, and she'll say all the time, 'It's just going to get worse.' I'm like, 'Great, thanks. That's really what I needed to hear.' But the reality is it's just going to get worse. And we've got to give small businesses around the world the ability to protect themselves.... [E]very small business [] actually has a heightened level of sensitivity right now to security issues because reality is if the small business gets hacked, they go out of business."[3]

[3] Morgan Stanley Technology Media & Telecom Conference, (Mar. 5, 2020), available at: https://research.alpha-sense.com?docid=T-CP_2346571&utm_source=alphasense%20platform&utm_medium=document%20share&utm_content=T-CP_2346571&utm_campaign=1620511695138.

34. SolarWinds' tactics worked. SolarWinds amassed a customer base of over 300,000 customers worldwide and obtained contracts with the United States government totaling more than $230 million. The Company's customers included (i) all five branches of the U.S. Military, (ii) the U.S. Pentagon, State Department, NASA, NSA, Postal Service, National Oceanic and Atmospheric Administration, Department of Justice, and the Office of the President of the United States, (iii) the FBI, Secret Service, National Nuclear Security Administration, Veterans Affairs, and the Department of Homeland Security, (iv) more than 425 of the U.S. Fortune 500 companies, (v) each of the top ten U.S. telecommunications companies, (vi) each of the top five U.S. accounting firms, and (vii) hundreds of universities and colleges across the world. As a result, by the second quarter of 2020, the Company was on track to generate $1 billion in revenue.

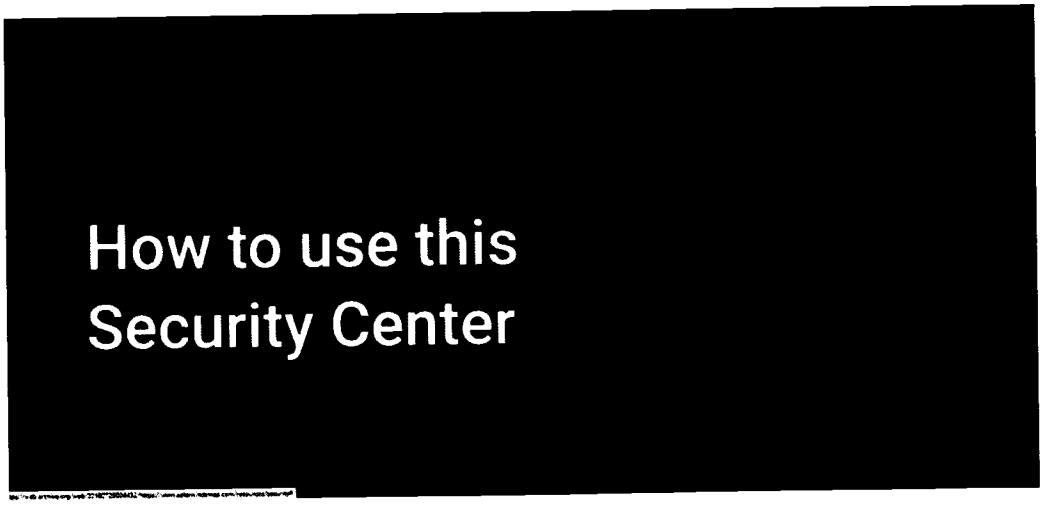
3. SolarWinds Assures Customers and Investors That It Adheres to Its "Security Statement"

35. Throughout the Class Period, SolarWinds and its executives represented to investors and customers that the Company adhered to specific security practices and prioritized cybersecurity. Over and over, the Company's executives—including its chief security spokesman, Defendant Brown—emphasized that the Company safeguarded the cybersecurity of its customers. These messages were reinforced by SolarWinds' executives during interviews, speeches at cybersecurity and IT summits, reports on their website, and during investor and analyst calls.

36. For example, in a March 14, 2019 SolarWinds podcast episode, Defendant Brown stated that "one of the things that we've focused on, that my team focuses on, is on heavy-duty hygiene." Yet again, in a September 10, 2020 blog post on SolarWinds' website entitled "Do Your Vendors Take Security Seriously?," Defendant Brown emphasized that the Company "places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards."

37. SolarWinds and its top executives detailed their purported adherence to critical cybersecurity practices in a formal Security Statement, which was first posted on or about August 28, 2018 on the Company's website. The Security Statement was reviewed and approved by Defendants Brown and Thompson and highlighted in the sections of the Company's website titled its "Security Center" (which was later renamed the "Trust Center"), where it was prominently posted. A link to access the Security Statement was included on every page of the Company's website. In its "Trust Center," SolarWinds assured customers and investors alike that the Company employed "[p]rocesses, procedures, and standards you can trust," explaining that customers' "security and privacy are our top priorities," and that the Company's "security strategy covers all aspects of our business."

38. Defendant Brown directly connected himself to the Security Statement, approved it, and adopted it. The Company's "Security Center," which featured the Security Statement, prominently included the below picture of Defendant Brown welcoming investors and customers to the "Security Center":



Additionally, when investors or customers visited the "Security Center," they were met with a video introducing and featuring Defendant Brown, in which he stated that "I'm excited to share

our new security resource center with everyone."

39. SolarWinds' top executives frequently directed investors and customers to the Company's website and, specifically, to its Security Center and Security Statement. For example, in Defendant Brown's article posted on the Company's website, "Do Your Vendors Take Security Seriously?," he emphasized the importance of company security statements, such as the SolarWinds "Security Statement," stating that "it's important your software vendors take their roles as business partners seriously. Their security *is* your security."[4] He stressed that "importantly, strong vendors *publish* their security protocols and processes so you can evaluate whether they meet your standards" and "reiterate[d] the point ... [that] your vendors should [] publish their policies and protocols." He emphasized the importance that a software company, such as SolarWinds, "places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards." He further directed investors and customers to the Company's Security Statement in its "Trust Center," telling readers that they "can learn all about the steps we take to protect your data by visiting our Trust Center today."

40. Once again, during an October 13, 2020 episode of the "Brown Report"—entitled "CyberSecurity in the New Different" and featuring Defendant Brown—investors and customers were directed to the Company's Security Statement in its Trust Center. Specifically, listeners were told to "[c]heck out the SolarWinds Trust Center for lots of good information on security, including our sponsored research, compliance and certification links, product information, and more. Visit solarwinds.com/trust-center." Similarly, during an August 25, 2020 episode of the Brown Report—entitled "Security Operations and IT Operations – Better Together"—after interviewing

[4] *N-Able*, "Do Your Vendors Take Security Seriously?" (Sept. 10, 2020), available at: https://www.n-able.com/blog/do-your-vendors-take-security-seriously#:~:text=The%20bottom%20line,publish%20their%20policies%20and%20protocols.

Defendant Brown, host Chris McManus directed investors and customers to the Company's Security Statement in its Trust Center once more. McManus advised, "[f]or a copy of the research that you heard throughout the episode and other useful security resources, be sure to visit SolarWinds Trust Center at solarwinds.com/trust-center."

41. The Company's other top executives similarly highlighted the information contained on the Company's website, including its Security and Trust Center. For example, during one investor conference, the Company's former Chief Financial Officer stated that the Company's "business model starts with the fact that we have to attract a lot of eyeballs to our website."[5] In December 2019, during a Company-sponsored "Analyst Day," Defendant Thompson likewise told analysts that the Company has "a lot of security products," and to learn about SolarWinds security, they should "go prowl our website."[6]

42. The SolarWinds Security Statement contained a series of representations about SolarWinds' purported adherence to cybersecurity practices, including each of the following:

43. ***The "Security Team."*** In the Security Statement, SolarWinds represented that the Company had a dedicated "security team" that "focuses on information security, global security auditing and compliance, as well as defining the security controls for protection of SolarWinds' hardware infrastructure." SolarWinds further stated that "[i]nformation security roles and responsibilities are defined within the organization" and represented that "[t]he security team receives information system security notifications on a regular basis and distributes security alert

---

[5] BAML Global Tech Conference (Jun. 5, 2019), available at: https://research.alpha-sense.com?docid=T-CP_2233793&utm_source=alphasense%20platform&utm_medium=document%20share&utm_content=T-CP_2233793&utm_campaign=1621900374173.

[6] Analyst Day (Dec. 11, 2019), available at: https://research.alpha-sense.com?docid=T-AS_2321141&utm_source=alphasense%20platform&utm_medium=document%20share&utm_content=T-AS_2321141&utm_campaign=1621900428110.

and advisory information to the organization on a routine basis after assessing the risk and impact as appropriate."

44. Cybersecurity experts have long recognized that maintaining a cybersecurity team—like the one SolarWinds assured investors and customers it had—is a critical component of cybersecurity. For example, McKinsey & Company explained in their comprehensive report on cybersecurity, titled "Perspectives on Transforming Cybersecurity," that "[t]o be effective[, an] organization needs a company-wide governance structure, built on a strong cyber-risk culture.... The cybersecurity unit should hold responsibility for cybersecurity company-wide, and ... be led by a senior, experienced CSO [chief security officer] with a direct reporting line to the board."[7] The cybersecurity firm Cygilant Security Monitoring, in its report titled "You Know You Need a Dedicated Cybersecurity Team, Now What?," similarly explained that "[o]ne of the most important steps in maturing your security program is moving to a dedicated team responsible for managing cyber risk."[8] SolarWinds assured investors that it maintained such a "security team."

45. ***"Information Security Policy."*** SolarWinds also represented to investors and customers in its Security Statement that the Company "maintains a written Information Security policy." The Company's "Information Security Policy" purportedly "cover[ed] a wide array of security related topics ranging from general standards with which every employee must comply, such as account, data, and physical security, to more specialized security standards covering internal applications and information systems." SolarWinds represented that it "receiv[ed] signed

---

[7] 24 Perspectives on Transforming Cybersecurity, MCKINSEY & COMPANY (Mar. 2019).

[8] *Cygilant Blog*, "You Know You Need a Dedicated Cybersecurity Team, Now What?" (Nov. 29, 2017), available at: https://blog.cygilant.com/blog/you-know-you-need-a-dedicated cybersecurity-team-now-what.

acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before providing authorized access to SolarWinds information systems."

46. These assurances were important to inspire consumer and investor trust. Cybersecurity experts have repeatedly recognized that it is imperative that an organization, such as SolarWinds, maintain and enforce compliance with an information security policy. For example, in its report "7 Cyber Security Best Practices Every Business Should Implement," Emazzanti Technologies explained that the primary cybersecurity best practice is to "create an acceptable use policy – and enforce it!"[9] Cybersecurity experts at Exabeam Security similarly stated in their report "The 8 Elements of an Information Security Policy" that "[o]rganizations large and small must create a comprehensive security program," emphasizing that "[c]reating an effective security policy and taking steps to ensure compliance is a critical step to prevent and mitigate security breaches."[10] SolarWinds and its executives assured investors that they maintained such an "Information Security Policy," and that the Company's employees had signed the acknowledgements attesting to their compliance with the policy.

47. ***Security Training***. SolarWinds further represented in its Security Statement that it required its employees to participate in "security training." On this subject, the Security Statement stated that its "[e]mployees are provided with security training as part of new hire orientation" and that "each SolarWinds employee is required to read, understand, and take a training course on the company's code of conduct." Defendant Brown also publicly emphasized the importance of "frequent security and compliance training," recognizing that it was a necessary component of any

[9] *Emazzanti Technologies*, "7 Cyber Security Best Practices Every Business Should Implement," (Dec. 5, 2019), available at: https://www.emazzanti.net/cybersecurity-best-practices/.

[10] *Exabeam*, "The 8 Elements of an Information Security Policy" (May 30, 2019), available at: https://www.exabeam.com/information-security/information-security-policy/.

effective cybersecurity program. In his statements to the public, he stressed that "[e]very employee should undergo periodic security and compliance training to make sure they're on guard against potential cyberthreats."[11]

48. Employee cybersecurity training—of the type Defendant Brown and SolarWinds told customers and investors they conducted—is a basic and necessary component of ensuring cybersecurity. In its report on cybersecurity, McKinsey & Company emphasized that companies must "build awareness campaigns and training programs, and adjust these regularly to cover the latest threats."[12] It further stressed that organizations must "provide comprehensive cybersecurity training to staffers at all levels."[13] Such training, McKinsey explained, ensures that "employees understand the rationale for cybersecurity protocols and raise their awareness. Even more important, it can signal to the business units that cybersecurity is a shared responsibility."[14] SolarWinds assured investors and customers that it conducted such security training.

49. ***The "Password Policy."*** SolarWinds also represented in its Security Statement that the Company's employees adhered to a strict password policy. The Company stated that "[o]ur password policy covers all applicable information systems, applications, and databases," with SolarWinds employing "password best practices [that] enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords." It further represented that its "[p]asswords are individually salted and hashed,"

---

[11] *N-Able*, "Do Your Vendors Take Security Seriously?" (Sept. 10, 2020), available at: https://www.n-able.com/blog/do-your-vendors-take-security-seriously#:~:text=The%20bottom%20line,publish%20their%20policies%20and%20protocols.

[12] *Perspectives on Transforming Cybersecurity*, MCKINSEY & COMPANY (Mar. 2019).

[13] *Id.* at 88.

[14] *Id.*

meaning that random, unique strings of characters are placed in the password, making each password unique.

50. SolarWinds emphasized the significance of these representations. For example, on May 19, 2019, the Company posted a SolarWinds authored report on its website titled "Password management – A quick best practice guide," in which the Company stated that "[e]ffective password management is a necessary evil when managing IT systems." The report further stated that "complex passwords" are "essential," as "[w]eak passwords give hackers an easy way into the infrastructure." In an April 28, 2020 SolarWinds authored report titled "5 Best Practices for Storing Company Passwords," the Company again stressed that "a password should be complex and at least eight characters in length," with "[s]pecial characters, like apostrophes and brackets [to] help add complexity and make it harder for hackers to guess passwords." The Company noted that passwords should not include "names, locations, or dates that might be easily guessed," that "different passwords [should be] used for each platform or account in use," and that "[a]s soon as an employee leaves, their passwords should be changed immediately across all platforms and accounts they had access to." The Company similarly stated, in a July 12, 2017 SolarWinds authored report on its website titled "Top Seven Reasons Why You Should Not Share Your Passwords," that, "[e]very time there is news of a new data breach and compromised user information, examples of … poor password behavior come to light."

51. Cybersecurity experts have recognized the critical importance of maintaining and enforcing a strict password policy, such as the one that SolarWinds told investors and customers that it followed. For example, the global cybersecurity software company Armor wrote in an article titled "Cybersecurity Best Practice: Password Management" that it is essential for organizations to implement a strict password policy because "a malicious individual can easily

guess [a weak password]. For as long as there have been passwords in the digital realm there have been password crackers.... They can rapidly run through a large set of possible character combinations or commonly used passwords in order to gain access to user accounts."[15] In addition, the SANS Institute, which specializes in information security, published a white paper entitled "Inadequate Password Policies Can Lead to Problems," confirming the obvious: "[p]assword policies are necessary to protect the confidentiality of information and the integrity of systems by keeping unauthorized users out of computer systems."[16] The SANS Institute similarly identified the following password attributes that should be specified by any basic password policy: "minimum length, allowed character set, disallowed strings (all numbers, dictionary words, variations of the username or ID), and the duration of use (expiration) of the password."[17]

52. ***"Limited" Authorization and Access.*** SolarWinds further represented to investors in its Security Statement that the Company restricted which of its employees could access its various databases. In a section of its Security Statement titled "Authentication and Authorization," the Company stated that SolarWinds employees are only "granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet" and that, beyond that, employees are only "granted access to certain additional resources based on their specific job function." The Company further assured investors and customers that it applied "Role-Based Access Controls," explaining that "[r]ole based access controls are implemented for access to information systems" and that "[a]ccess controls to sensitive data in [Company] databases,

---

[15] *Armor*, "Cybersecurity Best Practice: Password Management," (Feb. 26, 2019), available at: https://www.armor.com/resources/blog/cybersecurity-best-practice-password-management/.

[16] Hermens, Leonard, *Inadequate Password Policies Can Lead to Problems*, SANS INSTITUTE (Oct. 10, 2001).

[17] *Id.* at 3.

systems, and environments are set on a need-to-know/least privilege necessary basis." SolarWinds further emphasized that "[b]y default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need."

53. Defendants buttressed these representations with additional statements emphasizing the importance of restricting privileges and database access to a limited set of SolarWinds employees. In a December 5, 2019 SolarWinds authored report on its website, the Company explained that "[t]he act of access management is all about controlling user access, which includes tracking and changing authorizations as needed.... Access management systems are critical because they help bolster organization data security." SolarWinds further warned of the consequences of a failure to restrict user access: "[h]ackers often attempt to gain access to user profiles because if they can hack into privileged accounts, they will enjoy privileged access to the sensitive data on the server." Defendant Brown likewise recognized the significance of maintaining cybersecurity controls and, specifically, limiting user access. As he explained in an October 13, 2020 episode of the Brown Report, "a very high percentage of the actual breaches and actual exploits that we see that occur because of just cyber hygiene.... They occur because people don't have the basics in place. They occur because people have too many access rights to too many things."

54. SolarWinds' representations that the Company closely monitored user access were important to customers and investors. For years, cybersecurity experts have recognized that organizations must carefully restrict which employees have access to what databases. For example, the cybersecurity firm Twilio explained, in a report titled "Principle of Least Privilege: What, Why, and Best Practices," that "[o]ne of the most important moves" a company can make "in the effort to prevent fraud and network breaches" is "to enact an access control

policy."[18] Further, as cybersecurity experts at the Queensland University of Technology have explained, Role-Based Access Control, the method of access control to which SolarWinds assured investors it adhered, is critical for an organization to enforce internal security policies.[19] Strict adherence to these role-assignments is necessary for a company like SolarWinds to administer security as a whole to all users in a particular role, rather than on a user-by-user basis. SolarWinds comforted analysts and customers through its representations that it maintained tight role-based access controls, in which an administrator assigns rights and permissions to "roles" rather than individual users.

55. ***"Network Segmentation."*** SolarWinds additionally told investors and customers that the Company protected against cybersecurity attacks by segmenting its network—with users only able to access those segments of the Company's network that related to their roles. In particular, the Company represented in its Security Statement that SolarWinds "maintains separate development and production environments," with "network segmentation through the establishment of security zones that control the flow of network traffic."

56. SolarWinds stressed the importance of its "network segmentation" through additional statements to customers and investors. For example, in a report on its website titled "What is a Network Segment?," SolarWinds stated that "[b]y isolating aspects of business networks from one another—say, separating the resources employees need to do their jobs from payroll information—a network segment makes it possible to more effectively control who has access to what." SolarWinds explained that not only was such network segmentation "a must

---

[18] *Twiilio*, "Principle of Least Privilege: What, Why, and Best Practices" (Sept. 12, 2019), available at: https://www.twilio.com/blog/principle-of-least-privilege-details-best-practices.

[19] 3 Rhodes, Anthony & Cacelli, William A Review Paper: Role Based Access Control QUEENSLAND UNIVERSITY OF TECHNOLOGY.

when it comes to governing access internally, it can also help mitigate the threats from cyberattacks." The Company further explained that, if "bad actors compromise one part of a network, segmentation means they haven't compromised all of it." SolarWinds assured investors that its networks were segmented, as set forth in the Security Statement.

57. ***Adherence to the NIST Cybersecurity Framework.*** SolarWinds bolstered the specific representations in its Security Statement with the further assurance that the Company "follows the NIST [National Institute of Standards and Technology] Cybersecurity Framework." The NIST's Cybersecurity Framework requires that "[a]ccess to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions." It further mandates that "[t]he organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information and security-related duties and responsibilities consistent with related policies, procedures, and agreements." The NIST Cybersecurity Framework additionally requires that companies "[d]o a full, nationwide criminal background check … on all prospective employees."

58. Employee background checks are a necessary and important component to maintaining cybersecurity. As *Security Magazine* highlighted in their article, "Why Background Checks Have Become a Standard for Businesses Dealing with Sensitive Information," companies handling sensitive information—like SolarWinds—must perform background checks on prospective employees, including of their criminal histories, to "prevent future threats."

59. The Company's representation that it adhered to the NIST's cybersecurity requirements was a significant reason it was able to attract public and private sector clients. For instance, the Company touted in an October 8, 2019 press release that its products could "help[]

IT and security professionals encourage employees to set passwords in accordance with the National Institutes of Standards and Technology (NIST) guidelines for strong passwords." In a November 14, 2019 press release, the Company again highlighted, in a section of the release entitled "SolarWinds Solutions for Government," that "SolarWinds ... has hundreds of built-in automated compliance reports to meet the requirements of major auditing authorities, including [the] ... NIST."

60. Once again, in a May 9, 2019 post entitled "Information Security Framework Examples and Standards," SolarWinds described the NIST Cybersecurity Framework as "a solid [security] foundation for small organizations" and noted that "it's important to be familiar with these frameworks in order to better assess threat levels and security needs of your customers, and to understand if your own business is compliant." The Company represented that it could help its customers become compliant with the NIST Cybersecurity Framework: "Contact our team to ensure that your security framework complies with industry standards."

* * *

61. Investors credited the Company's representations in its Security Statement and assurances that SolarWinds prioritized cybersecurity. The representations enabled the Company to complete its initial public offering and sell over $375 million in Company stock at the start of the Class Period, as well as over $270 million in Company stock just months later. The Defendants also personally profited from taking the Company public, as well as the Company's soaring stock price achieved through its representations about its supposed cybersecurity practices and protections. Indeed, within a manner of months, the Company's stock price climbed from the IPO price of $15 to a Class Period high of $23.55—an increase of over 55%—and analysts noted the Company's "compounding growth story that is unique in software." During that period, Defendant

Thompson sold over $20 million in personal stock. For their part, the Private Equity Firms sold $261 million in shares in a May 2019 follow-on offering. Then, they sold another $460 million in shares on December 7, 2020—just one week before SolarWinds' stock price plummeted when investors learned the truth, discussed further below, about the Company's deficient cybersecurity controls.

B. Unknown to Investors at the Time, SolarWinds' Internal Security Was in Shambles and the Company Did Not Adhere To Its Security Statement

62. While the Company trumpeted its commitment to cybersecurity and the representations in its Security Statement, SolarWinds and the Private Equity Firms that controlled it relegated cybersecurity to the back of the line as a result of their focus on cost-cutting to achieve near-term gains. Unknown to investors at the time, the Company's Global Cybersecurity Strategist told the Company's top executives shortly before the Class Period that SolarWinds devoted insufficient resources and attention to cybersecurity, exposing the Company and its customers to an inevitable cybersecurity attack. Yet the Company refused to reform, leading him to resign in protest. As a result, the Company's cybersecurity failures went unabated. These failures were made patently clear when the Company learned in late-2019 that its confidential password for its internal Company databases had been publicly available for years and then, just twelve months later, when it was revealed that the Company's cybersecurity deficiencies led to the biggest cybersecurity breach in U.S. history.

1. SolarWinds Executives Were Told About the Company's Deficient Cybersecurity Controls

63. Defendants knew or, at minimum, were severely reckless in not knowing, that the Company did not comply with its Security Statement or adhere to the cybersecurity commitments it touted. Shortly before the Class Period, Ian Thornton-Trump—SolarWinds' Global

Cybersecurity Strategist—forcefully alerted the Company and its executives to its cybersecurity deficiencies. Lead Counsel interviewed Mr. Thornton-Trump in connection with its investigation.

64. Mr. Thornton-Trump joined SolarWinds in early 2017, when the Company acquired LogicNow, a U.K.-based cloud computing company. Mr. Thornton-Trump was a 15-year veteran in the cybersecurity industry and served in the Canadian Forces' Military Intelligence Branch as a Criminal Intelligence Analyst. He previously worked as a cybersecurity analyst for multinational insurance, banking and health-care companies. He was the Global Cybersecurity Strategist for SolarWinds after its acquisition of LogicNow.

65. Mr. Thornton-Trump recounted to Lead Counsel that SolarWinds' security was not as robust as it needed to be, especially since it was doing business with the U.S. government. Mr. Thornton-Trump further explained that SolarWinds misrepresented its security to customers. He told Lead Counsel that the Company had no security leadership and no centralized way of dealing with security at the corporate level. There was no company culture around IT, and responsibilities were uncoordinated.

66. Mr. Thornton-Trump stated that he learned upon joining SolarWinds that "[t]here was no corporate security" at SolarWinds and no dedicated security positions at all at SolarWinds. He assumed a multi-billion-dollar company like SolarWinds would have security personnel, but he was surprised to learn when he spoke with SolarWinds upon joining the Company that they did not have any security people. Among other things, Mr. Thornton-Trump stated that, at SolarWinds, there was no Chief Information Security Officer ("CISO")—a standard security position at software companies handling customer data. He further explained that there was no one centrally coordinating security efforts at SolarWinds. He also stated that, in addition to lacking a corporate security department, "[t]here was a lack of security at the technical product level,"

meaning that there was no process for ensuring the Company's software products were secure. The absence of a security team was especially surprising to Mr. Thornton-Trump given the fact that the risk of the Company being hacked was known: "We knew in 2015 that hackers were looking for any route into a business. But SolarWinds did not adapt. That's the tragedy."

67. Mr. Thornton-Trump identified other critical deficiencies in cybersecurity at SolarWinds. When he specifically asked his colleagues at SolarWinds for documentation regarding cybersecurity—in particular regarding the security of SolarWinds' computing environment and data protection policies and controls—he was not able to obtain any such documentation. "I never saw it, and I did ask for it," Mr. Thornton-Trump stated. He reiterated to Lead Counsel that he never saw any written information security policy at the Company, despite his asking to see one.

68. Mr. Thornton-Trump added that that there was no cybersecurity awareness education or training at SolarWinds. He described how he did not receive any such training at SolarWinds, and he was unaware of any security trainings for its employees.

69. Mr. Thornton-Trump also observed that the Company was not protecting its employees' computers from attack. He explained that, at SolarWinds, workstation vulnerability management was not effective. Many people were running out-of-date software, which he knew because he saw the workstations of several of his colleagues; their web browsers were out-of-date, and a lot of employees were running with "extraordinary rights" on their computers.

70. The Company also did not limit user access controls on the Company's critical networks, which exposed the Company's "crown jewels." Mr. Thornton-Trump explained that there appeared to be no restrictions or controls in place regarding network segmentation at the Company. He described how SolarWinds development engineers should have been segmented

from the rest of the network with heightened security, but that was not occurring at SolarWinds. To the contrary, SolarWinds was using a "flat" network, which meant anyone could connect to any server in the network. "It's bad practice," Mr. Thornton-Trump explained. He described how, rather than allow a very small group of people access to the Company's "crown jewels," it was a free-for-all at SolarWinds. Mr. Thornton-Trump further explained that the "extraordinary rights" employees had on their computers meant that anyone could download and install software without it being centrally managed or properly licensed. Mr. Thornton-Trump stated that the developer environment was even more "free-wheeling" than the general computing environment, and that the Company failed to rigorously enforce the segregation of the developer environment and production environments.

71. The Company also did not follow any password policies, and employees used highly vulnerable passwords that could easily be guessed. For example, Mr. Thornton-Trump recounted that the Company did not use multi-factor authentication for passwords.[20] He further recounted that, for the development portions of the network, there was no password change policy—meaning that passwords could remain the same indefinitely. In fact, some of the passwords in the development unit of the business were "hard-coded," such that they could never be changed; if the passwords were changed, the product would stop working. Mr. Thornton-Trump also explained that, for many of the Company's database backends, default passwords were used.

[20] Multi-factor Authentication is an authentication method that requires the user to provide two or more verification factors to gain access. At the same time that it failed to implement multi-factor authentication, the Company publicly stressed its importance in preventing security breaches. For instance, in a December 18, 2019 article entitled "What is Two-Factor Authentication," the Company wrote, "2019 was a banner year for cybersecurity threats in both quantity and complexity.... MSPs need the right tools to secure their customers' IT infrastructure. Two-factor authentication can keep end users safe from data breaches on a day-to-day basis."

Indeed, every single SolarWinds Orion install had default passwords, which Mr. Thornton-Trump explained was a problem.

72. Based on his work at the Company and review of its practices, Mr. Thornton-Trump concluded that, "from a security perspective, SolarWinds was an incredibly easy target to hack."

73. Mr. Thornton-Trump voiced his concerns to the Company's executives. When his concerns were not taken seriously, Mr. Thornton-Trump decided that he needed to make the case more forcefully for security at SolarWinds. In advance of doing so, Mr. Thornton-Trump conducted approximately one month of research, "digging pretty deep" and speaking to people about active attacks in the cybersecurity space.

74. On or about April 22, 2017, Mr. Thornton-Trump convened a meeting with several of the Company's top executives. Attendees at the meeting included SolarWinds' Chief Technology Officer, Joe Kim; Chief Information Officer, Rani Johnson; and Chief Marketing Officer, Gerardo Dada. Mr. Kim and Mr. Dada reported directly to Defendant Thompson. At the meeting, Mr. Thornton-Trump presented a PowerPoint presentation titled "Creating Security."

75. In his PowerPoint presentation, which Lead Counsel has reviewed, Mr. Thornton-Trump stressed to the Company's executives that "We need to be good cyber security citizens," explaining that a "data breach is bad for us and bad for our customers." Mr. Thornton-Trump warned of several deficiencies necessary to address in order to "Create Security" at SolarWinds. Mr. Thornton-Trump started his presentation by warning the Company's executives that, with regard to cybersecurity, there was "No centralized reporting," "No centralized management," and "Silos of communication"—issues that needed to be addressed to create security at the Company.

76. To remedy these problems, Mr. Thornton-Trump explained to the Company's executives that SolarWinds needed to develop a security team. Specifically, he told them that, at

minimum, the Company needed to hire a Chief Information Security Officer, a Senior Director of Cyber Security, and two Portfolio Security Managers. Mr. Thornton-Trump explained that the two "Portfolio Security Managers (PSM) are required to create and implement a security roadmap for solution compliance and solution security."

77. Developing a security team was not simply intended to achieve efficiency. Mr. Thornton-Trump stressed that these positions were necessary to avoid a catastrophic cyberattack. As he explained in his Presentation, SolarWinds' "infrastructure and corporate systems exist in a precarious state." Mr. Thornton-Trump further told the Company's executives that this precarious state, if not rectified, would result in another cyberattack. As he reminded his colleagues, the Company had already been subjected to the "Apache Struts" compromise, a damaging security breach in 2017 during which "cyber criminals quickly exploited" and compromised "over 500 customer systems."

78. Mr. Thornton-Trump made clear to the Company's executives that hiring security experts would not be enough to cure the Company's deficiencies. The Company also needed to commit culturally to upholding the cybersecurity standards it publicly espoused. Mr. Thornton-Trump stressed to the SolarWinds executives during his presentation that they should change the culture so that security became a core value—a statement that received "a lot of nodding." Mr. Thornton-Trump further told the Company's executives that the Company needed to "motivate participation, engagement, and loyalty" among its employees to promote internal security. He emphasized to the Company's executives that they needed to, among other things, establish security training modules for the Company's employees, as well as implement an internal scoring system that would rate the Company's security practices on a scale from "needs improvement" to "exceeds best practices."

79. During his Presentation, Mr. Thornton-Trump also stressed to the Company's executives that SolarWinds needed to adopt an Internal Security Message Plan to answer the question: How would the Company react in the event of a significant data breach? Mr. Thornton-Trump noted in his "Creating Security" presentation that any company that provided information technology services to third-parties—such as SolarWinds—is "already a security brand" and thus must have a robust plan in the event of a cyberattack. Mr. Thornton-Trump further spelled out the "link" between the Company's commitment to security and its bottom-line: "[S]ecure solutions and a secure company provides revenue and sustains the business."

80. Mr. Thornton-Trump's Presentation made abundantly clear that the Company failed to adhere to cybersecurity best practices, and significant and immediate reform was necessary. The Presentation specifically stated that a commitment to cybersecurity was essential to the Company's continued existence. He made his point bluntly, stating: "The survival of our customers depends on a commitment to build secure solutions" and "The survival of the company depends on an internal commitment to security."

81. Mr. Thornton-Trump recounted to Lead Counsel that the executives in attendance at his Presentation all agreed with his assessment of the Company's security and what needed to be done to remedy the situation. The meeting was not adversarial, and there was no dissenting opinion. Mr. Thornton-Trump added that the SolarWinds executives in attendance knew cybersecurity was a problem at SolarWinds and knew that the problem was getting worse.

82. Mr. Thornton-Trump further recounted to Lead Counsel that, at the meeting, none of the SolarWinds executives in attendance could answer the question of who owned security over the Company's development operations. Mr. Thornton-Trump explained that SolarWinds did not have any security operations over development. And when Mr. Thornton-Trump asked the

Company's Chief Technology Officer for insights on these matters, Joe Kim admitted to him that "[w]e're just not there yet."

83. Mr. Thornton-Trump explained that he saw his Presentation to the Company's executives as an opportunity to save the Company, as he said it was "clear as day" that a cyberattack was coming. He reiterated that he made it clear to the Company's executives that the Company lacked the necessary safeguards, and they needed to change the culture; but, it was like trying to build a house on a patch of dirt—there was "no foundation," he stated.

84. Mr. Thornton-Trump's Presentation to the Company's executives was widely discussed internally within SolarWinds. SolarWinds Former Employee ("FE") 1 said it was not a big secret at the Company that Mr. Thornton-Trump "was saying bold things."[21] FE 1 confirmed that he knew that Mr. Thornton-Trump had a high-level meeting about his cybersecurity concerns. FE 1 further learned the message of Mr. Thornton-Trump's presentation: "that SolarWinds as a collective entity was not investing enough in security in order to make sure something bad doesn't happen." FE 1, who viewed slides from Thornton-Trump's presentation, confirmed that the statements Mr. Thornton-Trump made in the PowerPoint slides that he saw were correct statements. FE 1 stated that he agreed and completely believed that SolarWinds was not making security a core tenet of anything that was being done based on how the Company was prioritizing.

2. SolarWinds Refuses to Reform, Causing Its Global Cybersecurity Strategist to Resign in Protest

85. SolarWinds' executives did not follow Mr. Thornton-Trump's directives to address cybersecurity. The Company's CEO, Defendant Thompson, did not want to spend money on the

[21] FE 1 was a Senior Director of MSP Evangelism at SolarWinds from September 2017 until September 2019. His work included strategy consultation for M&As with the leadership team. FE 1 worked as the CEO of an information technology consulting company for 15 years prior to starting at SolarWinds.

Company's cybersecurity. Mr. Thornton-Trump explained that, when he delivered his Presentation, he was met with resistance as to costs because that was the corporate culture at SolarWinds. Gerardo Dada and Joe Kim both told Mr. Thornton-Trump at the time that Defendant Thompson did not like spending money, even on security. Mr. Thornton-Trump also recalled an attendee of the Presentation stating that "Kevin [Thompson] won't like spending that kind of money"—a statement that none of the other SolarWinds executives in attendance disagreed with. "Everyone understood the risk [of not addressing cybersecurity] and saw my passion, but it just wasn't going to happen," Mr. Thornton-Trump added.

86. After the conclusion of his "Creating Security" presentation, Mr. Thornton-Trump was notified that the Company's senior leadership was, indeed, not interested in spending the money to implement the necessary changes outlined in the Presentation.

87. Mr. Thornton-Trump resigned in protest. He explained that he did not want to be put in a position where he was asked to say something publicly about SolarWinds' cybersecurity that was not the truth. He described the reason for his resignation from the Company as follows: "You either live in that state of cognitive dissonance, or you fix the problem, or you [get] yourself out of the situation." Mr. Thornton-Trump also conveyed the reasons for his departure at the time to his fellow SolarWinds executives, including Gerardo Dada (SolarWinds' Chief Marketing Officer), John Pagliuca (Executive Vice President & General Manager, SolarWinds MSP), and Alistair Forbes (Managing Director, SolarWinds MSP).

88. On May 15, 2017, Mr. Thornton-Trump emailed Mr. Dada, about the reasons for his resignation. He wrote that "[u]nfortunately … the current SW [Solar Winds] MSP leadership is … unwilling to make the corrections necessary," which Mr. Thornton-Trump noted was "[a] point I made in my briefing to the CIO [i.e., the Chief Information Officer]." He explained that

he had "lost faith in the leadership" of the Company, and that it was "too painful to watch from the sidelines as mistake after mistake unfolded."

89. Mr. Dada did not disagree with Mr. Thornton-Trump's assessment of the Company's failures. To the contrary, he responded within hours to Mr. Thornton-Trump's email by explaining that he "agree[d] with [his] assessment and ... appreciate[d] the effort and candor [he] put behind trying to do the right thing at SolarWinds."

90. Mr. Thornton-Trump's account has been corroborated by other former SolarWinds employees. These employees' accounts confirm that the Company did not take the steps necessary to rectify its deficient cybersecurity practices during the Class Period.

91. For example, when asked if SolarWinds improved their security practices when the Company went public at the start of the Class Period, FE 2 laughed and emphatically said, "No"—it was the "same sh*t, different day."[22] FE 2 agreed that the culture at SolarWinds was very much about cost-cutting and not about ensuring SolarWinds complied with basic cybersecurity. FE 2 interacted with Defendant Thompson, who never spoke about the Company's internal cybersecurity; the focus was always sales, money, or profitability. FE 2 explained that security trainings did not exist at SolarWinds. FE 2 additionally explained that he could personally attest to the fact that employees that were not in SolarWinds' development operations division could, nevertheless, access parts of the development operations' system. He knew this because he did it himself. As a sales engineer, he should not have had that access, he explained. He confirmed that

[22] FE 2 was a sales engineer at SolarWinds from November 2014 until July 2019. FE 2 provided technical assistance to several Fortune 500 clients with security, network management, and system products, as well as led product demonstrations for potential customers. Prior to starting at SolarWinds, FE 2 worked as an engineer at a telecommunications company and provided information technology support to a prominent investment bank.

there was an absence of limitations on user access. He added that, at his current company, what he can touch is very tightly regulated and controlled; this control did not exist at SolarWinds.

92. FE 3 confirmed that SolarWinds employees could download files onto their computers at the Company without authorization, in contrast to other companies where they try to lock down what employees can download onto their computers without authorization.[23] FE 3 recalled that his SolarWinds colleagues downloaded files onto their computers, and he stated that "there was latitude there" at SolarWinds. FE 3 further stated that he could not recall ever taking a security training course at SolarWinds. When asked if SolarWinds was prioritizing cybersecurity when he was at the Company, FE 3 said, "Clearly they [we]re not actively talking with us about it, so I would say [they were not]."

93. Similarly, FE 4 stated that, even after SolarWinds became public at the start of the Class Period, nothing changed with respect to security.[24] FE 4 further stated that, during his entire tenure with SolarWinds—from 2016 to June 2020—there was not a time when anyone at the Company spoke with him about maintaining good cybersecurity. There were no policies that he saw, no training, and he never signed any documents regarding cybersecurity (e.g., affirmations that he would adhere to any cybersecurity policies).

94. FE 5 also recounted that SolarWinds never did any internal cybersecurity training with the Company's staff.[25] FE 5 contrasted this with his current company, in which they have

[23] FE 3 was a Security Specialist at SolarWinds from December 2018 until June 2019. He was responsible for selling one of the Company's security-related products.

[24] FE 4 was a backup and disaster recovery specialist at SolarWinds from 2016 to June 2020. FE 4's duties included being a combination salesperson/sales engineer for the Company's backup and disaster recovery product. He demoed the product for customers and helped onboard customers into utilizing the solution.

[25] FE 5 was a director of global recruiting at SolarWinds from September 2018 to February 2020. He managed recruiting for senior level roles at the Company while leading a team of Global

someone who is actively engaged to do cybersecurity with its employees. FE 5 further explained that, at SolarWinds, employees were never instructed to change passwords, either. This lack of attention to security surprised FE 5 because he was used to having those types of security safeguards from his prior employment. FE 5 confirmed that he never did any cybersecurity training at SolarWinds. FE 5 stated that he found it really weird that a publicly-traded company never did routine cybersecurity training for their employees.

95. FE 5 further stated that, when new employees joined the Company, there was no cybersecurity agreement that they had to sign, and FE 5 stated that he never signed any such agreement in his time at the Company. FE 5 added that there was no cybersecurity team at SolarWinds, stating that, "If there was one, they had a really plush job because they didn't do anything." FE 5 explained there was "no emphasis whatsoever" on cybersecurity at SolarWinds.

96. FE 5 further explained that the Company also did not even do background checks on candidates for any employment position—a failure that he was also surprised to see. FE 5's understanding was that the Company was not performing background checks because the Company did not want to spend the money to perform them. FE 5 further stated that he heard from candidates all the time that SolarWinds was the place to go if you have a criminal record. FE 5 was spearheading the effort to implement background checks for employment candidates, but the reform still was not implemented by the time he left the Company in February 2020.

97. FE 6 confirmed that SolarWinds did not do background checks on new hires, and it was a general concern that they were not being done.[26] FE 6 further stated that he was concerned

---

Corporate Recruiters. FE 5 has an extensive background in recruiting, both in the private sector and public sector.

[26] FE 6 was a HR business partner contractor at SolarWinds from August 2016 to March 2019. He worked at the Company's headquarters. He reported to Melissa Garza, the Vice President of Human Resources.

that background checks were not being done, and even though recruiting was game to do it, it was not being supported or funded. FE 6 also stated that he could not recall any onboarding training or other training relating to cybersecurity at the Company.

98. FE 7 confirmed that there was no security training at SolarWinds.[27] He stated that the only training he received at SolarWinds was how to sell the product. FE 7 contrasted this to his current employer, where he has training on information security and how to keep information secure. FE 7 further stated that he could not recall any information security policy at SolarWinds. FE 7 added that he was never told about a security team at the Company and stated that, if such a team existed, he believed he would have interfaced with them. FE 7 added that, at SolarWinds, computers were left open and unlocked at the end of the day, and laptops were left out on desks or in public areas like the snack area.

99. FE 8 also confirmed that there was no security training at all at the Company, which he found ironic because the Company was acquiring and launching cybersecurity products when the Company had no cybersecurity on their own front end to protect themselves.[28] He explained that it was common knowledge at the Company that SolarWinds did not use their own security products that they were selling and promoting.[29] FE 8 confirmed that "solarwinds123" was a commonly used password at the Company. FE 8 stated that it was common knowledge at the Company that "solarwinds123" was the Company's default password. He recalled that it was the

---

[27] FE 7 was a Security Account Manager at SolarWinds from June 2017 until June 2019. FE 7 specialized in managing the Company's security-focused products – such as Access Rights Manager and Threat Monitor – and maintaining customer relationships with respect to those products. FE 7 has previous experience working at other technology companies.

[28] FE 8 worked at the Company from June 2018 until May 2019 as a Marketing Associate. He worked in the Company's headquarters.

[29] Mr. Thornton-Trump similarly noted that the Company was "not eating their own dog food," which meant they were selling solutions that they were not using themselves.

WiFi password as well as the default password for other interfaces, and that it was used for the Company's marketing automation system Marketo.

100. FE 9 similarly confirmed that there was no cybersecurity training at the Company during his tenure at the Company—from 2016 until March 2021.[30] He stated that the Company did not appear to be security aware at all; that there was a "total lack of security" internally; and that the Company was "not very security conscious." He found it surprising that the Company did not have multi-factor authentication in place and was not enforcing it, and stated that the Company did not implement two-factor authentication on the Salesforce software platform until after the breach in December 2020. FE 9 stated that, at SolarWinds, he saw a Company that was focused on revenue rather than development and security. He was not surprised when the breach occurred.

101. FE 10 confirmed that there were no information security trainings at SolarWinds.[31] He confirmed that he looked back through the documents he was given when he was onboarded and saw nothing about internal information security. He further confirmed that he received no cybersecurity training and could not find or remember being given or signing an information security policy. He further stated that the Company was pretty open with giving access to employees on their network, in contrast to his time at a previous employer. He recalled being able to access files via the Company's intranet that were above his level, and he never saw any restrictions on Company computers. He described employees' access to the network as a "free for all." FE 10 further confirmed that employees could download things onto Company computers without authorization.

---

[30] FE 9 was a Sales Engineer at the Company from 2016, when the Company acquired his then-employer LogicNOW, until March 2021.

[31] FE 10 was an employee in the Customer Retention group, where he worked in Renewal Sales at the Company's headquarters. He worked at the Company from March 2020 until December 2020, and has worked in the IT space for 18 years.

102. FE 1 additionally explained that, after Mr. Thornton-Trump's departure from SolarWinds, there was no radical change to address Mr. Thornton-Trump's concerns. FE 1 stated that he completely believed that SolarWinds was not making security a core tenet of anything that was being done, based on how the Company was prioritizing at the time. He said it was an accurate interpretation to say that Defendant Thompson never said anything about focusing on internal cybersecurity measures at any point after Mr. Thornton-Trump left. FE 1 further explained that he participated in strategy meetings with Defendant Thompson, including quarterly business reviews ("QBRs"). Defendant Thompson attended and described the Company's priorities during some of those QBRs, including during a meeting in January 2018 in Austin and a meeting in January 2019 in Durham, North Carolina. FE 1 could not recall a time when Defendant Thompson spoke about internal cybersecurity as a priority, and could recall no mention by Defendant Thompson of prioritizing building internal cybersecurity.

3. SolarWinds Is Told That the Password To Access Its Internal Update Server Was Publicly Available On the Internet For Years

103. The grave consequences of SolarWinds' failure to adhere to its cybersecurity commitments were made even more apparent on November 11, 2019. On that date, a researcher, unaffiliated with SolarWinds, notified SolarWinds in writing that the Company's confidential password to access, modify, and add files to its Update Server was publicly available on a website. Worse yet, the password, as well as a link to access the Company's internal update server, had been publicly available on the web for approximately one-and-a-half years.

104. By way of background, SolarWinds—like most software companies—maintains an update server on its website (the "Update Server"). SolarWinds directs customers to visit the Update Server to download updates to the Company software that the customers purchased. SolarWinds employees need a password to access and add files to the Update Server for download

by the Company's customers. It is critical that the password to the Company's internal server to add files to the Update Server is kept confidential and secure, so as to avoid unwanted or malicious materials being added to the Update Server for download by customers.

105. Unknown to customers and investors at the time, the Company's Update Server was compromised for nearly a year-and-a-half. Indeed, on June 17, 2018, a SolarWinds employee posted to the popular public website GitHub the credentials and link that allowed anyone to enter SolarWinds' internal systems containing the update files that the Company instructed its customers to download on its Update Server. The GitHub website is commonly used by software developers to share computer code and other information related to software development. By accessing SolarWinds' internal system using the password and credentials on the GitHub website, any malicious actor could add malware to any of the update files that the Company sent out to its tens-of-thousands of customers, including U.S. federal agencies.

106. On November 19, 2019, Vinoth Kumar notified SolarWinds in writing of this critical compromise to its Update Server. Mr. Kumar is a software engineer who specializes in security. He currently works as the Security Lead at the company HealthifyMe. Prior to that, he worked as a Senior Development Engineer at the company Grofers and as a Senior Software Development Engineer at the company Zomato.

107. Mr. Kumar notified SolarWinds on November 19, 2019 that he "found a public GitHub repo [i.e., website] which [is] leaking ftp credentials belong[ing] to SolarWinds." He directed the Company to a link to the public GitHub webpage that contained the user credentials. The webpage provided a link to the Company's internal connection to the Update Server, as well as the "confidential" username and password to access the internal server. With these credentials, Mr. Kumar (or anyone) could upload malware or any other file to the Company's Update Server,

which would then be included in the Company's regular software updates downloaded by SolarWinds' customers.

108. To underscore the significance of the Company's cybersecurity failure, Mr. Kumar demonstrated to SolarWinds that he had utilized the compromised username and password, entered the Company's Update Server, and uploaded a file onto the Update Server. The file that Mr. Kumar uploaded would, absent remediation, be included in any updates downloaded by SolarWinds' customers. Mr. Kumar made the point abundantly clear in his email to the Company, in which he stated that "any hacker could [have] upload[ed] malicious [files]" to the Update Server.

109. Mr. Kumar's email to SolarWinds included the Company's password for its internal access to the Update Server. The password was "solarwinds123," a remarkably vulnerable password that violated basic password policies. As Defendant Thompson has since admitted, the Company tasked an intern to set the password for this critical server. The Company's new CEO has further admitted that, worse yet, the Company's intern set the password for this critical server in 2017—meaning that it remained unchanged, and the operative password for this critical Company server, for over two years.

110. The implications of the Company's public dissemination of its password to its Update Server were plain. Mr. Kumar later recounted to *Reuters* that "anyone could access SolarWinds' update server by using the password 'solarwinds123.'"[32] After entering the Company's internal server, any malicious actor could insert malware into any of the updates

[32] *Reuters,* "Hackers used SolarWinds' dominance against it in sprawling spy campaign," (Dec. 15, 2020), available at: https://www.reuters.com/article/global-cyber-solarwinds/hackers-used-solarwinds-dominance-against-it-in-sprawling-spy-campaign-idUSKBN28Q07P.

downloaded by SolarWinds' customers. Mr. Kumar explained to *Reuters*, "'[t]his could have been done by any attacker, easily.'"[33]

111. Making matters worse, throughout the Class Period, SolarWinds instructed customers to disable their antivirus software when they downloaded updates from SolarWinds' Update Server. Specifically, SolarWinds instructed customers on its website to "exclude from antivirus scanning" all SolarWinds "Orion Platform products."[34] As a result, customers were exposed to viruses and malware when they updated their software updates through the Company's Update Server. Cybersecurity expert Costin Raiu confirmed SolarWinds' instruction to customers to disable their scanners before downloading updates to SolarWinds' products.[35] Mr. Raiu explained that SolarWinds "advis[ed] users to DISABLE antivirus scanning for [SolarWinds'] Orion products' folders"—a practice he accurately described as "nuts."[36]

112. Defendant Brown admitted in recent interviews in March 2021 that he and SolarWinds were informed about the issues raised in Mr. Kumar's email. Recognizing the significance of the issue, Defendant Brown stated that he and SolarWinds—within an hour of being notified by Mr. Kumar—changed the password for the server. He has acknowledged his contemporaneous knowledge of the issue, stating that "we"—i.e., Brown and SolarWinds—"fixed [the issue] within the same hour it was reported." Meanwhile, investors and customers were kept

---

[33] *Id.*

[34] Ian Thornton-Trump confirmed that the Company told customers to disable their antivirus software when installing SolarWinds product—a "common practice at the Company."

[35] Costin Raiu is a Director of Global Research a Kaspersky Lab. He is a security researcher with more than 20 years of experience in the antivirus industry. He works on new threat defense technologies, next generation endpoint security, targeted attacks protection, threat intelligence, and reverse engineering.

[36] *Bloomberg*, "SolarWinds Adviser Warned of Lax Security Years Before Hack," (Dec. 21, 2020), available at: https://www.bloomberg.com/news/articles/2020-12-21/solarwinds-adviser-warned-of-lax-security-years-before-hack.

in the dark. No action was taken to advise investors that the Company's Update Server had been compromised for over a year. Nor did SolarWinds tell investors at that time—or at any other time during the Class Period—that the Company failed to adhere to the password policy and the other aspects of the Security Statement that it assured investors it closely followed.

4. SolarWinds Lacked the Cybersecurity Protections That It Represented in Its Security Statement

113. Numerous former SolarWinds employees have confirmed that the Company's representations to customers and investors about the Company's cybersecurity were false and misleading. As *The New York Times* later explained, SolarWinds' "former employees and advisers" knew that "SolarWinds was a ripe target [for a cybersecurity attack] not only for the breadth and depth of its software, but for its own dubious security precautions."[37] *Bloomberg News* similarly reported that "several cybersecurity researchers ... discovered what they described as glaring security lapses at the company."[38] Indeed, contrary to its public representations, SolarWinds failed to adhere to the representations in its Security Statement, exposing its customers to a cyberattack and investors to major losses.

114. ***SolarWinds had no "Security Team."*** As discussed above, the Company's Security Statement assured investors that SolarWinds employed a dedicated "security team," with "[i]nformation security roles and responsibilities ... defined within the organization." But, in truth, the Company lacked any such "security team." Mr. Thornton-Trump has explained that "[t]here was no corporate security [at SolarWinds]. No one that appeared to own it and no one that

---

[37] *The New York Times,* "Billions Spent on U.S. Defenses Failed to Detect Giant Russian Hack," (Dec. 16, 2020), available at: https://www.nytimes.com/2020/12/16/us/politics/russia-hack-putin-trump-biden.html.

[38] *Bloomberg,* "SolarWinds Adviser Warned of Lax Security Years Before Hack," (Dec. 21, 2020), available at: https://www.bloomberg.com/news/articles/2020-12-21/solarwinds-adviser-warned-of-lax-security-years-before-hack.

appeared to be responsible for it." He further explained that security roles were not defined within the organization; the Company had no security leadership, no security team, and no centralized way of dealing with security at a corporate level. He additionally recounted how there was no company culture around IT, and responsibilities were uncoordinated. When asked about the Security Statement's references to a "security team," he responded that there was no security team at SolarWinds.

115. Other reports have confirmed that SolarWinds lacked the "security team" described in its Security Statement. FE 2 confirmed that, during his six years at the Company, he never once heard of a "security team" being at the Company. He stated that, if he had a security problem at SolarWinds, he would not have even known who to contact. FE 4 likewise stated that, in the nearly six years he worked at the Company, he never heard of a security team at SolarWinds. FE 5 confirmed that there was no cybersecurity team at SolarWinds, stating that, "If there was one, they had a really plush job because they didn't do anything." FE 7 confirmed that he was never told about a security team at the Company and stated that, if such a team existed, he believed he would have interfaced with them. FE 6 confirmed that he was not aware of any security team at SolarWinds. Additionally, *The New York Times* noted, in its December 16, 2020 exposé, that the Company did not even have a chief information security officer during the Class Period—which is the executive position at software companies tasked with overseeing cybersecurity.

116. ***SolarWinds had no "Security Information Policy."*** As discussed above, SolarWinds also represented in its Security Statement that it maintained a Security Information Policy and, even more, required its employees to review and sign such a policy. In truth, no such policy existed, and SolarWinds employees were never required to sign such a policy.

117. Mr. Thornton-Trump explained that there was no documentation that he received that discussed SolarWinds' data protection policies or controls. "I never saw it, and I did ask for it," Thornton-Trump stated. He further stated that he never signed any form related to cybersecurity. He reiterated that he never saw any written information security policy at the Company, and he had asked for one. He also noted that SolarWinds' contractors were never subject to any requirement that they sign any sort of acknowledgements before plugging into the Company's network.

118. Accounts of other SolarWinds employees are in accord. FE 2 stated that he went back and read the Company's entire employee manual on a couple of occasions in 2019, and there was not any information about a security policy in the employee manual. He did not recall ever receiving a security policy at SolarWinds; nor did he recall being required to sign any such policy, including at the time he was hired. FE 4 likewise stated that in his nearly six years at the Company he never saw or received a written information security policy, and never had to sign any document about cybersecurity. FE 4 added that internal security was "never really talked about" at SolarWinds. FE 5 confirmed that, when new employees joined the Company, there was no cybersecurity agreement that they had to sign, and FE 5 stated that he never signed any such agreement in his time at the Company. FE 5 further confirmed that there was "no emphasis whatsoever" on cybersecurity at the Company. FE 10 confirmed that he looked back through the documents he was given when he was onboarded and saw nothing about internal information security. He further confirmed that he could not find or remember being given or signing an information security policy.

119. ***SolarWinds did not follow its "Password Policy."*** As discussed above, Defendants assured investors that the Company followed a strict password policy, with the Company

purportedly employing "password best practices [that] enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords." SolarWinds further claimed that its passwords were "individually salted and hashed," meaning passwords used at the Company were unique. In truth, the Company did not have a "password policy" and did not employ "password best practices."

120. Multiple former employees of the Company have confirmed that the Company neither maintained nor adhered to a password policy. FE 4 explained that there was no password policy at SolarWinds. FE 2 similarly explained that he never received any direction from the Company about maintaining appropriate passwords, and SolarWinds never provided any formal trainings about secure passwords. He could recall no instruction or policies for passwords during the nearly five years that he worked at the Company.

121. Nor did the Company require individual passwords or periodic changes to passwords. Mr. Thornton-Trump recounted that, at SolarWinds, some of the passwords in development were hard-coded, such that they could never be changed. He explained that the Company's use of hard-coded passwords made SolarWinds a "soft target" for a cyberattack. Additionally, Mr. Thornton-Trump stated that every SolarWinds Orion install had default passwords. He explained that this posed a problem because, if they are not changed at the time of install, it is trivial for someone from another organization to access your system. FE 5 also recounted that, at SolarWinds, employees were never instructed to change their passwords.

122. Moreover, the Company's employees used weak passwords that were extremely vulnerable to cyberattack. FE 2 explained that "solarwinds123" was a common password used at the Company. FE 2 recounted that there were lab environments in which sales engineers could demonstrate products for customers, and frequently there was only one shared common password,

with "solarwinds123" being the default password. FE 2 further explained that the password "solarwinds123" could not be changed because it was a shared password; accordingly, if it changed, others would be locked out of the lab. FE 7 confirmed that "solarwinds123" was a common default password at the Company, including the original password for his Company-provided laptop. FE 8 also confirmed that "solarwinds123" was a commonly used password at the Company, and it was common knowledge at the Company that "solarwinds123" was the Company's default password. He recalled that it was the WiFi password as well as the default password for other interfaces, and that it was used for the marketing automation system Marketo.

123. Mr. Thornton-Trump likewise stated that he was informed by colleagues that "solarwinds123" was a commonly used password at SolarWinds. And, as discussed above, this same "solarwinds123" password was the Company's password for employees to access its internal server for its critical Update Server—a password that went unchanged for two years.

124. In addition to failing to follow its password policy, the Company's critical passwords were not kept confidential. The "solarwinds123" password for the Company's internal Update Server was publicly available on the Internet for over one-and-a-half years, as discussed above. Additionally, employees' individual passwords were also shared publicly—also on the Internet website GitHub. As *The New York Times* reported in its exposé, it was shown internal SolarWinds emails demonstrating "that [SolarWinds] employees' passwords were leaking out on GitHub [in 2019]."

125. ***SolarWinds did not provide cybersecurity training to its employees***. SolarWinds also falsely represented in its Security Statement that the Company provided its employees with cybersecurity training. Mr. Thornton-Trump explained that, while he was at the Company, there

was no cybersecurity awareness education or training at SolarWinds. He was unaware of any security trainings for employees, and he did not receive any such training at SolarWinds.

126. Nor did the Company start providing cybersecurity training after he left. FE 2, who was with the Company from 2014 until July 2019, stated that security trainings did not exist at SolarWinds; there was also no cybersecurity training at SolarWinds during his time at the Company. He contrasted this with both his current and prior employers, who provided scheduled and repeated security trainings. FE 2 further stated that cybersecurity was not emphasized at SolarWinds.

127. FE 4 similarly stated that there was no security training at SolarWinds. He reiterated that there was not a time during his entire tenure with SolarWinds—from 2016 to June 2020—when anyone at the Company even spoke with him about maintaining good cybersecurity. Meanwhile, he stated that employees would have benefited from information security training.

128. FE 5 also confirmed that SolarWinds never did any internal cybersecurity training with staff, which FE 5 stated he found really weird. He contrasted SolarWinds with his current employer, who has someone who is actively engaged to do cybersecurity with employees. FE 5 stated that SolarWinds' lack of attention to security surprised him.

129. FE 7 also confirmed that there was no security training at SolarWinds. He stated that the only training he received at SolarWinds was how to sell the product. FE 7 contrasted this to his current employer, where he has training on information security and how to keep information secure.

130. FE 6 likewise confirmed that he did not recall any onboarding training or other training about cybersecurity. FE 3 confirmed that he also could not recall ever receiving a security training course at SolarWinds. FE 9 similarly confirmed that there was no cybersecurity training

at the Company during his tenure at the Company—from 2016 until March 2021. FE 10 further confirmed that he received no cybersecurity training at the Company. Finally, FE 8 also confirmed that there was no security training at all at the Company.

131. ***SolarWinds did not segment its network and did not limit user authorization.*** The Company's Security Statement also falsely assured investors that SolarWinds restricted employees' access with the Company's network, which was supposedly "segmented" in order to prevent and mitigate harm in the event of a cyberattack. In truth, SolarWinds employees were allowed unfettered access to critical databases and information areas, and the Company's network was not segmented.

132. Multiple witnesses have confirmed that the Company did not impose necessary limits on employees' access within the Company's network. Mr. Thornton-Trump explained that the workspace for development engineers should have been segmented with heightened security, but that was not occurring at SolarWinds. He explained that the Company was using a "flat" network, which meant anyone could connect to any server in the network. "It's bad practice," Mr. Thornton-Trump explained. Mr. Thornton-Trump confirmed that best practice is to allow only a very small group of people to access "the crown jewels," but it was a free-for-all at SolarWinds. Mr. Thornton-Trump added: "How easy would it be for the bad guys to get in? My contention was, very easy, because the basic ways to detect them were not there." He explained the benefits of network segmentation: If the network were segmented, you could identify when a person was trying to break into a segment of the network.

133. FE 2 stated that, while he was at the Company, employees who were not in development operations could also access parts of the development operations system. He knew this because he did so personally. As a sales engineer, he should not have had that access, he

explained. He confirmed that there was an absence of limitations on user access. He added that, at his current company, what he can touch is very tightly regulated and controlled; this control did not exist at SolarWinds, he explained.

134. When asked if there were controls over where users could look within the SolarWinds network, FE 4 explained that he could view other products that he did not work on and there were no restrictions. FE 3 also confirmed that SolarWinds employees could download files onto their computers at the Company without authorization, in contrast to other companies where they try to lock down what employees can download onto their computers without authorization. FE 3 recalled that his SolarWinds colleagues downloaded files onto their computers, and he stated that "there was latitude there" at SolarWinds.

135. Similarly, FE 10 stated that the Company was pretty open with giving access to employees on their network, in contrast to his time at a previous employer. He recalled being able to access files via the Company's intranet that were above his level, and he never saw any restrictions on Company computers. He described employees' access to the network as a "free for all." FE 10 further confirmed that employees could download things onto Company computers without authorization.

136. These witness accounts are further corroborated by the fact, discussed above (*see* ¶109), that the Company allowed a temporary employee, an intern, to access one of the Company's most critical servers—its Update Server—and, even more, authorized him to set the confidential password for this critical Update Server.

137. ***SolarWinds did not perform background checks on its employees.*** The Company's Security Statement also falsely assured investors that Company "follows the NIST [National Institute of Standards and Technology] Cybersecurity Framework," which includes a

requirement to conduct background checks. Multiple witnesses have explained that the Company did not conduct background checks of potential employees.

138. FE 5, the Company's director of global recruiting, explained that the Company did not do background checks on candidates for any employment position—a failure that he was also surprised to see. FE 5's understanding was that the Company was not performing background checks because the Company did not want to spend the money to perform them. FE 5 further stated that he heard from job candidates all the time that SolarWinds was the place to go if you have a criminal record. FE 5 was spearheading the effort to implement background checks for employment candidates, but the reform still was not implemented by the time he left the Company in February 2020.

139. FE 6, who also worked in human resources at SolarWinds, confirmed that SolarWinds did not do background checks on new hires, and it was a general concern that they were not being done. FE 6 further stated that he was concerned that background checks were not being done. FE 6 added that, even though recruiting was game to do background checks, it was not being supported or funded.

140. ***SolarWinds did not prioritize cybersecurity.*** As discussed above, SolarWinds publicly assured customers and investors that "security and privacy are our top priorities." In truth, the Company never prioritized cybersecurity, exposing customers and investors to the consequences of SolarWinds' deficient cybersecurity practices. Multiple witnesses have explained that SolarWinds and Defendant Thompson singularly focused on cost-cutting and short-term profits, not cybersecurity.

141. For example, Mr. Thornton-Trump explained to Lead Counsel that, when he delivered his Presentation outlining the Company's cybersecurity deficiencies, he was met with

resistance as to costs because that was the corporate culture at SolarWinds. Company executives Gerardo Dada and Joe Kim both told Mr. Thornton-Trump at the time that Defendant Thompson did not like spending money, even on security, and an attendee of the Presentation stated that "Kevin [Thompson] won't like spending that kind of money"—a statement which none of the other SolarWinds executives in attendance disagreed with. Additionally, after Mr. Thornton-Trump's Presentation, the Company's senior leadership notified him that the Company's leadership was, indeed, not interested in spending the money to implement the necessary changes outlined in his "Creating Security" presentation—a result that caused Mr. Thornton-Trump to "lose faith" in the Company's leadership and resign.

142. FE 1 agreed and believed that SolarWinds was not making security a core tenet of anything that was being done based on how the Company was prioritizing. FE 1 explained that he attended approximately ten to twelve QBRs. Defendant Thompson would attend some of these QBRs and, when he attended, delivered a corporate message where he described the priorities of the corporation. FE 1 specifically recalled Defendant Thompson attending QBR meetings in January 2018 in Austin and in January 2019 at the Durham office. FE 1 could not recall a single instance when Defendant Thompson spoke about how internal cybersecurity was a priority during the QBRs. FE 1 also could not recall a time when internal cybersecurity was brought up during any all-hands quarterly meetings led by Thompson. He recalled no mention of prioritizing building internal cybersecurity by Defendant Thompson. FE 1 described the lack of focus on security as a "sin of omission."

143. FE 7 also confirmed that internal cybersecurity was not discussed by Defendant Thompson during the QBRs. FE 7 added that computers were left open and unlocked at the end of the day and laptops were left out on desks or in public areas like the snack area.

144. FE 5 confirmed that internal cybersecurity was not mentioned as a priority during the all-hands quarterly meetings typically led by Defendant Thompson. He stated that there was "no emphasis whatsoever" on cybersecurity at the Company.

145. Similarly, when asked if SolarWinds was prioritizing cybersecurity when he was at the Company, FE 3 said, "Clearly they [we]re not actively talking with us about it, so I would say [they were not]."

146. Finally, FE 9 stated that the Company did not appear to be security aware at all, that there was a "total lack of security" internally, and that the company was "not very security conscious." He found it surprising that the Company did not appear to be security aware at all, and he was not surprised when the breach occurred. FE 9 stated that, at SolarWinds, he saw a Company that was focused on revenue rather than development and security.

147. Former SolarWinds employees interviewed by major media outlets have also confirmed that the Company did not prioritize cybersecurity. For example, *The New York Times* reported in January 2021 that "[i]nterviews with current and former employees of SolarWinds suggest it was slow to make security a priority, even as its software was adopted by America's premier cybersecurity company and federal agencies."[39] These employees further told *The New York Times* that, when Defendant Thompson became CEO, "every part of the business was examined for cost savings and common security practices were eschewed because of their expense."[40] Additionally, a former SolarWinds software engineer interviewed by *Bloomberg* explained that SolarWinds "prioritize[d] the development of new software products over internal

[39] *The New York Times,* "As Understanding of Russian Hacking Grows, So Does Alarm," (Jan. 2, 2021), available at: https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

[40] *Id.*

cybersecurity defenses."[41] The employee, who requested anonymity due to having signed a non-disclosure agreement, said "it wasn't uncommon for some of the company's computer systems to be operating out-of-date web browsers and operating systems, which could make them more vulnerable to hackers."[42] Meanwhile, as Defendant Brown has admitted publicly, using out-of-date web browsers violates basic cybersecurity: "Guess what? If you are running an out-of-date … operating system … they are going to take it over and throw ransomware on it," he has explained.[43]

148. Further prioritizing cost-cutting over cybersecurity, Defendant Thompson moved the Company's engineering offices to locations notorious for cybercrime. As *The New York Times* explained in its January 2021 report, Defendant Thompson put SolarWinds' "customers at greater risk for attack" by "mov[ing] much of [SolarWinds'] engineering to satellite offices in the Czech Republic, Poland and Belarus, where engineers had broad access to the Orion network management software."[44] Professor Terry Thompson of John Hopkins University reiterated that "the company put itself at risk by outsourcing its software development to Eastern Europe, including a company in Belarus. Russian operatives have been known to use companies in former Soviet satellite countries to insert malware into software supply chains."[45] Cybersecurity expert

---

[41] *Bloomberg,* "SolarWinds Adviser Warned of Lax Security Years Before Hack," (Dec. 21, 2020), available at: https://www.bloomberg.com/news/articles/2020-12-21/solarwinds-adviser-warned-of-lax-security-years-before-hack.

[42] *Id.*

[43] Sept. 10, 2019 Interview, "Mid-town Mr. Brown on SECURITY that MATTERS!," available at: https://www.youtube.com/watch?v=uet2dl2PYyg.

[44] *The New York Times,* "As Understanding of Russian Hacking Grows, So Does Alarm," (Jan. 2, 2021), available at: https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

[45] *The Conversation,* "The SolarWinds hack was all but inevitable – why national cyber defense is a 'wicked' problem and what can be done about it," (February 9,2021), available at:

Paul Joyal echoed that SolarWinds' "use of foreign-owned offshore companies to provide software engineering [was] a great threat."[46]

149. Defendant Thompson engaged in his cost-cutting strategy to appease the Private Equity Firms that controlled SolarWinds. Thoma Bravo's "take-private, then public" approach to SolarWinds involved reducing operating costs—including by "flattening the organization structure" and "scop[ing] out consolidation options in a company's vertical"—to expand revenue exponentially.[47] The Private Equity Firms and SolarWinds leadership refused to make the necessary expenditures and commitment to cybersecurity because it delivered no short-term profit. As Matt Stoller, a former Senior Policy Advisor to the Senate Budget Committee, explained, the Private Equity Firms' corporate strategy of cost-cutting contributed to the Company's inattention to cybersecurity and, ultimately, the cyberattack at SolarWinds: "the same sloppy and corrupt practices that allowed [the] massive cybersecurity hack made [Thoma Bravo CEO Orlando] Bravo a billionaire."[48] He added that, by choosing to forego those cybersecurity safeguards, SolarWinds turned "other people's risk into profit." Stoller further observed that "[i]t's not a coincidence that SolarWinds head of security [Ian Thornton-Trump] warned of a looming catastrophe, and quit after he was ignored."[49]

---

https://theconversation.com/the-solarwinds-hack-was-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem-and-what-can-be-done-about-it-153084.

[46] *Security Infowatch,* "More questions than answers as SolarWinds breach probe expands," (Jan. 19, 2021), available at: https://www.securityinfowatch.com/cybersecurity/article/21206223/more-questions-than-answers-as-solarwinds-breach-probe-expands.

[47] *Buyouts*, "Top fundraiser Thoma Bravo bets software's red -hot run is far from over," (Jan. 4, 2021), available at: https://www.buyoutsinsider.com/top-fundraiser-thoma-bravo-bets-softwares-red-hot-run-is-far-from-over/.

[48] *BIG by Matt Stoller,* "How to Get Rich Sabotaging Nuclear Weapons Facilities," (Jan. 3, 2021), available at: https://mattstoller.substack.com/p/how-to-get-rich-sabotaging-nuclear.

[49] *Id.*

C. Customers and Investors Learn That SolarWinds Fails To Maintain Cybersecurity

150. On Sunday, December 13, 2020, a series of media reports revealed that cybercriminals had inserted malware into updates for SolarWinds software. A United States government official identified the SolarWinds breach as "the worst hacking case in the history of America."[50]

151. SolarWinds did not disclose the breach; rather, reports of the breach first emerged via reporting by *Reuters*. The Company's infected software updates were downloaded by customers for over six months and by tens-of-thousands of SolarWinds' customers, including U.S. government agencies and Fortune 500 companies. Once downloaded by SolarWinds' customers, the infected software enabled the cybercriminals to spy on SolarWinds' customers. The cybercriminals could access SolarWinds' customers' classified documents, review their private emails, and obtain their trade secrets.

152. Worse yet, the Company has now admitted that the cybercriminals entered the Company's network as early as January 2019—*i.e.*, nearly two years earlier and before Mr. Kumar notified the Company of the compromised password for SolarWinds Update Server.

153. Over the subsequent days and weeks following the revelation of the SolarWinds breach on December 13, 2020, reports emerged further demonstrating SolarWinds' deficient cybersecurity controls. Indeed, on December 13, 2020, the Cybersecurity and Infrastructure Security Agency ("CISA") released an emergency directive ordering all federal civilian agencies to immediately disconnect from their networks all SolarWinds Orion products. The CISA

[50] *Las Vegas Review-Journal*, "Cyber attack may be 'worst hacking case in the history of America,'" (Dec. 17, 2020), available at: https://www.reviewjournal.com/news/politics-and-government/cyber-attack-may-be-worst-hacking-case-in-the-history-of-america-2223270/.

emergency directive—one of only five such emergency directives issued in seven years—tied the emergency measure directly to the Company's deficient cybersecurity practices, stating that the vulnerability in the SolarWinds product "poses unacceptable risks to the security of federal networks."

154. These reports led cybersecurity experts to conclude—correctly—that the Company's deficient cybersecurity controls made SolarWinds an attractive and easy target for, and led to, the cybersecurity breach.

155. Moody's announced on December 14, 2020 that it was reviewing SolarWinds for a potential downgrade of the Company's credit rating following "the announcement that SolarWinds has been made aware of a cyberattack that inserted a vulnerability within its Orion monitoring products." As Moody's wrote, the revelation of the Company's deficient cybersecurity practices "could "result[] in reputational damage, a material loss of customers, slowdown in business performance, or high remediation and legal costs."

156. SolarWinds' stock began to plummet, with analysts tying the drops to the Company's deficient cybersecurity practices. For instance, on December 14, 2020, the Company's stock fell 17%, from $23.55 at the close of the prior trading day to $19.62 on December 14, 2020. Analysts immediately tied the precipitous stock drop to SolarWinds' deficiencies. As Barclays wrote, "This morning, SolarWinds put out a press release acknowledging that its Orion software platform was targeted in potentially broad-reaching cyberattacks .... We highlight that [SolarWinds] Orion suite is the integrated SolarWinds platform across its core IT products ... [which] made up 45% of its total revenue ytd [year-to-date] across all customers .... Overall, we believe shares will remain under pressure as investors worry about potential financial and legal impacts to the company and as the events continue to unfold." Jefferies concurred, writing, "Key

Takeaway: SWI was down 17% after it announced a security compromise that impacts the Orion NM product. The bad news is that the fed govt., a major vertical, has frozen the software and that this event will have an impact on revs. and new deals...."

157. On December 15, 2020, public reports emerged that (as discussed above at ¶¶103-12) the password to access the Company's Update Server was "solarwinds123" and had been on a public website for a year-and-a-half. Cybersecurity experts recognized that the Company exhibited deficient cybersecurity controls by (1) allowing its employees to utilize the password "solarwinds123" for its internal Update Server; (2) never changing the password for over two years; (3) authorizing an intern to set this critical password and access the Update Server; and (4) enabling the password to enter the public domain for over one-and-a-half years.

158. SolarWinds' use of the password "solarwinds123" for a critical server was, as Professor Terry Thompson explained, "an egregious violation of fundamental standards of cybersecurity."[51] SolarWinds' explanation—that the password was set by an intern—further demonstrated the Company's failure to adhere to basic cybersecurity practices. As the executive director of security at Okta, Marc Rogers, explained, "[i]n placing blame on an intern for setting a production password in 2017 ... SolarWinds revealed deep, systemic cybersecurity failures at many levels of the organization.... That intern's ability to set a password of 'solarwinds123' on a critical production system highlights fundamental problems with password policy, systems management and auditing.... All of these failures suggest an organization rife with systemic security issues, an ineffective security management program, and a lack of technical controls or

[51] *The Conversation,* "The SolarWinds hack was all but inevitable – why national cyber defense is a 'wicked' problem and what can be done about it," (Feb. 9, 2021), available at: https://theconversation.com/the-solarwinds-hack-was-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem-and-what-can-be-done-about-it-153084.

compliance with industry standards."[52] Rogers further commented that organizations, such as SolarWinds, "that allow junior employees privileged access to production systems like this are typically a 'Wild West' when it comes to controlling access for all systems, not just one."[53]

159. Next, on December 15, 2020 reports emerged that, as a result of its cybersecurity deficiencies, SolarWinds did not remove the infected SolarWinds software updates from its Update Server even after it learned that its software updates were infected with malware and downloaded by customers. In an article titled "SolarWinds Cyber Attacks Raise Questions About The Company's Security Practices And Liability," *Forbes* contributor and CEO of Global Cyber Risk, Jody Westby, summed up the news succinctly: "Andrew Morris of GreyNoise Intelligence reported online that he had been able to download the infected installer from SolarWinds website and 'found that the backdoor'd DLL [Dynamic Linked Library] is definitely still contained in the installer on the [SolarWinds] website literally right now.' My God."[54] As Ms. Westby explained, "We have waited long enough for companies to devote adequate attention and resources to cybersecurity programs. This is the consequence. We must do better .... or the bad guys will win. It really is that simple."[55] The fact that SolarWinds—even after learning that its updates contained

---

[52] *SC Media*, "SolarWinds blaming intern for leaked password is symptom of 'security failures'" (Mar. 2, 2021), available at: https://www.scmagazine.com/access-control/solarwinds-blaming-intern-for-leaked-password-is-symptom-of-security-failures/.

[53] *Id.*

[54] *Forbes,* "SolarWinds Cyber Attacks Raise Questions About The Company's Security Practices And Liability," (Dec. 16, 2020), available at: https://www.google.com/search?q=SolarWinds+Cyber+Attacks+Raise+Questions+About+The+Company%E2%80%99s+Security+Practices+And+Liability+forbes&oq=SolarWinds+Cyber+Attacks+Raise+Questions+About+The+Company%E2%80%99s+Security+Practices+And+Liability+forbes&aqs=chrome..69i57.1722j0j4&sourceid=chrome&ie=UTF-8.

[55] *Id.*

malware—failed to remove the infected files from its Update Server further demonstrated an utter lack of cybersecurity controls.

160. On December 15, 2020, the Company's stock tumbled another 8%, from $19.62 on December 14, 2020 to $18.06 on December 15, 2020 on heavy trading volume, in direct response to the further revelations regarding the Company's deficient cybersecurity practices, with shocked analysts tying the drop directly to the continuing revelations. For instance, RBC Capital Markets wrote that, "While the situation is fluid, our view is that the cyber-attack introduces an incremental reputational risk to the story and around fourth quarter new business and renewal opportunities. As such, we believe shares are likely to remain under pressure in the near-term...." RBC Capital Markets lowered its price estimate on SolarWinds' stock "as we will look to gather additional details" on the breach.

161. On December 17, 2020, further details of the Company's deficient cybersecurity and resultant breach emerged. Microsoft President Brad Smith revealed that more than 40 of its customers were victims of the attack. Five large information technology companies, including Deloitte, also announced they were breached as a result of SolarWinds' cybersecurity deficiencies. *Bloomberg* reported that at least three state governments were also compromised, and that the cybercriminals had also infiltrated the Department of Energy and the National Nuclear Security Administration—the source of the United States' nuclear codes.

162. On December 17, 2020, SolarWinds' stock plummeted a further 19% in direct response to the further revelations, from $17.60 on December 17, 2020 to $14.18 on December 18, 2020 on heavy trading volume, with analysts tying the stock's freefall directly to the mounting news about the Company's deficient cybersecurity. Wedbush wrote in a December 18, 2020 report: "To put it bluntly, based on all the initial data and speaking with our Beltway contacts last

night/today we believe this cyber-attack will likely rank as one of the worst (very possibly the worst ever) in the last decade given the targeted and cyber espionage nature of this attack." Jefferies, in a December 21, 2020 report, concurred: "SWI has lost 40% of its value or ~3B over the past wk [week].... [W]e believe this is the worst hack for a software company .... The hack will in all likelihood have an impact on results next year."

163. On December 21, 2020, reports emerged containing first-hand accounts of current and former SolarWinds employees. These reports further confirmed and documented the deficiencies in the Company's cybersecurity controls. These reports contained statements by Mr. Thornton-Trump, including that internal security deficiencies rendered the Company an "easy target to hack." Commentators took note, such as Jake Williams, a former employee of the NSA. He explained that security deficiencies were an "underlying problem" at SolarWinds that remained because SolarWinds viewed "'[s]ecurity is a cost center, not a profit center.'"[56] As Professor Terry Thompson explained, "SolarWinds, driven by its growth strategy and plans to spin off its managed service provider business in 2021, bears much of the responsibility for the damage." David Corchado of Investis Digital echoed that the breach should serve as a "wake-up call" that SolarWinds had deficient security practices.[57]

164. Market analysts also took note of the revelations of the Company's deficient cybersecurity. For instance, on December 21, 2020, Truist downgraded their recommendation for

[56] *Bloomberg*, "SolarWinds Adviser Warned of Lax Security Years Before Hack," (Dec. 21, 2020), available at: https://www.bloomberg.com/news/articles/2020-12-21/solarwinds-adviser-warned-of-lax-security-years-before-hack.

[57] *Investisdigital*, "Why the Cybercrime of the Century Is a Wake-Up Call for Businesses," (Jan. 13, 2021), available at: https://www.investisdigital.com/blog/technology/solarwinds-cybercrime-wake-call-to-businesses-cybersecurity.

SolarWinds from "Buy" to "Hold," and reduced the share price target by $12.[58] In addition, Jeffries lowered its SolarWinds revenue estimates for 2021 by over $100 million, and lowered its 2022 estimates by approximately $50 million.

165. The fallout from the cybersecurity breach has been immense. Thomas Bossert, the homeland security adviser to President Trump and the deputy homeland security adviser to George W. Bush, wrote in *The New York Times* that "[t]he magnitude of this ongoing attack is hard to overstate." Mr. Bossert wrote that SolarWinds allowed the cybercriminals "persistent access" to the networks they infiltrated, meaning they could continue to access the networks. As he wrote, "The remediation effort alone will be staggering. It will require the segregated replacement of entire enclaves of computers, network hardware and servers across vast federal and corporate networks."

166. Numerous customers have abandoned the Company's software. One of SolarWinds' major customers, Mimecast, announced in March 2021 that it was dropping SolarWinds in favor of Cisco, a competitor that offers a similar product. Since the revelation of SolarWinds' deficient security practices, customers' trust in the Company has eroded. For the first quarter of 2021, license revenue declined by 33% compared to the first quarter of 2020, with the decrease in renewals led by federal agency customers.

167. SolarWinds' investors have also suffered immensely as a result of the Company's failures to adhere to the cybersecurity practices it assured them it followed. The Company's stock price has not recovered, and analysts have continued to reduce their price targets for the

[58] In two separate reports, dated February 25, 2021 and April 29, 2021, respectively, Truist has maintained its downgraded recommendation.

Company's shares.[59] SolarWinds has now become the laughingstock of the software industry, with popular t-shirts sold on the internet bearing the slogan "SolarWinds123: Made by Interns, Insecure by Design," and cybersecurity experts routinely chastising the Company in articles, lectures, and talks for failing to adhere to basic cybersecurity.

D. SolarWinds Is Forced To Admit It Lacked Sufficient Security Measures During the Class Period

168. The Company has replaced Defendant Thompson and instituted several reforms. SolarWinds and its new CEO, Sudhakar Ramakrishna, have assured customers and investors that they will now implement the reforms necessary to address cybersecurity. These belated changes, dubbed the "Secure by Design" initiative, further make clear that the Company lacked the security practices that it had assured its customers and investors it had implemented during the Class Period.

169. Cybersecurity experts have correctly viewed the Company's belated adoption of these security measures as an admission that its cybersecurity was deficient from the start. As NPR wrote, "the overhaul of SolarWinds' security practices add up to an admission that something was wrong." Mr. Thornton-Trump similarly observed, "[i]f I come up with an 11-point plan to improve my company's security one interpretation of that could be .... that there were at least 11 material deficiencies in the actual security we had. I see that the 11-point plan is actually an admission that things were not good in this security house." And the Company's new CEO, when asked if the Company could "do thing[s] better" on the cybersecurity front, admitted, "[a]bsolutely."

170. In announcing the Secure by Design initiative, the Company's new CEO stated that the Company was "reflecting on our own security practices and seeking opportunities to enhance

[59] During January and February 2021, JPMorgan, Barclays, Evercore ISI and Credit Suisse all reduced their share price targets for the Company.

our posture and policies." To that end, CEO Ramakrishna added that he would work "directly with the SolarWinds team to lead the immediate improvement of critical business and product development systems, with the goal of making SolarWinds an enterprise software industry security leader." The Secure by Design initiative implicated several of the deficient security practices that persisted at SolarWinds throughout the Class Period, including those discussed below.

171. ***"Security Team" and Prioritizing Security.*** The Company is now finally investing in developing a "security team" of the type that it had previously assured investors that it already had. As discussed above, numerous witnesses have recounted that the Company lacked a "security team" during the Class Period. Among other things, the Company lacked a Chief Information Security Officer—a shortcoming identified by Ian Thornton-Trump four years ago and highlighted by *The New York Times* in its recent exposé. The Company's new CEO has finally created the position of Chief Information Security Officer at SolarWinds—an independent officer of the Company devoted to security. As reported by TechRepublic, in a March 2021 article titled "SolarWinds CEO Gives Chief Security Officer Authority and Air Cover to Make Software Security A Priority," the Company's new CEO has created this new position to uphold its stated commitments, with the Company now "creat[ing] a seat at the table" for an executive focused on cybersecurity.

172. In a further belated commitment to prioritize cybersecurity, the Company has created a Technology and Cybersecurity Committee of its Board of Directors (the "Cybersecurity Committee"). The Cybersecurity Committee will "assist the Board in fulfilling its oversight responsibilities with respect to the Company's ... information technology systems and cybersecurity generally." Comprised of three Company directors, the Cybersecurity Committee meets to "[p]rovid[e] guidance to the Board on the Company's cybersecurity and other IT risks,

controls and procedures and the Company's strategy to mitigate cybersecurity risks and potential breaches," "[r]eview[] and provid[e] guidance to the Board on the integrity of the Company's IT systems' operational controls to ensure legal and regulatory compliance," and "[r]eview[] ... the Company's disaster recovery capabilities."

173. ***Password management***. The Company further admitted as part of its Secure by Design Initiative that the Company would start "[r]eviewing all accounts, updating all passwords and turning up the level of conditional access" in its network. The Company also admitted that it now would start to "[r]equire the use of multi-factor authentication" to protect against weak passwords. These changes were necessary because, as discussed above, the Company did not previously have a password policy, and it allowed its employees to routinely use stale, default passwords—such as "solarwinds123"—including for critical aspects of its network.

174. ***Limited Access Privileges***. The Company further admitted in its Secure by Design Initiative that it would start "consistently enforcing least privileges policies for ALL employees." This "initiative" further confirmed the falsity of the Company's prior representations, contradicting its Class Period representations in its Security Statement that it already granted employees "a limited set of default permissions to access company resources" and only did so "based on their specific job function." The Company's Secure by Design Initiative was necessary precisely because, unknown to investors during the Class Period, the Company provided employees access to SolarWinds resources unrelated to their job functions, putting the Company, its customers, and its shareholders at risk.

175. ***Network Segmentation.*** The Company further admitted through its Secure by Design Initiative that, notwithstanding its prior representations, it did not segment its network during the Class Period. Indeed, as part of its Secure by Design Initiative, the Company, going

forward, will begin "[l]ocking down access to our environments." This change was necessary because, as discussed above, the Company did not previously segment its networks; users were able during the Class Period to access areas of the network unrelated to their job function.

176. ***Additional changes.*** As discussed above (*see* ¶111), SolarWinds instructed its customers during the Class Period to disable antivirus software before uploading files from its Update Server—a practice that cybersecurity experts referred to as "nuts." SolarWinds' new management itself has recognized that this practice was improper. *Bloomberg* has reported that "[t]he SolarWinds's web page [recommending customers disable their antivirus software] has been subsequently removed from public view" after the cybersecurity breach occurred—an effective admission that the instruction never should have been given in the first place.

E. The SEC, Department of Justice, State Attorneys General Launch Investigations Into SolarWinds, But the Company Still Pays Its Executives Lavishly

177. The Company's misconduct is currently under investigation. In its 2020 Form 10-K, the Company admitted that it was facing "numerous investigations and inquiries by domestic and foreign law enforcement and other governmental authorities … including … the Department of Justice, the Securities and Exchange Commission, and various state Attorneys General." The Company also faces inquiries under privacy regulations such as the European Union's General Data Protection Regulation.

178. The Company has also recognized the sustained impact from the revelations of its deficient cybersecurity controls. The Company has stated that it is "reasonably possible that we could incur losses associated with these proceedings and investigations" and that the fallout from the revelations may "have a negative impact on employee morale" and result in the "diversion of management's attention from the operation of our business." In addition, the Company has estimated that remediation efforts will cost $20 million to $25 million annually.

179. However, despite the fallout from the Company's deficient cybersecurity practices, the Company continued to pay lavish bonuses to its former executives—much to the amazement of market analysts and investors. As one analyst noted, "SolarWinds paid its top leaders more than $65 million in total [during 2020] despite a colossal breach that exposed 18,000 customers." These payments included $23.9 million in awards to Defendant Thompson and $8.8 million to the Company's former Chief Technology Officer, Joe Kim—one of the multiple executives who Mr. Thornton-Trump urged to adopt the directives in his "Creating Security" presentation.[60] Moreover, market observers have noted that "SolarWinds agreed to pay Thompson an additional $312,500 ... to help the company defend itself in investigations" even though "Thompson led the firm from the time the hackers got a foothold in the [SolarWinds] Orion software through when news of the attack went public."

V. ADDITIONAL ALLEGATIONS OF SCIENTER

180. A host of facts, including and in addition to those discussed above, support a strong inference that Defendants knew, or, at minimum, were severely reckless in not knowing, the true undisclosed facts about SolarWinds' deficient cybersecurity controls when they made their false or misleading representations to investors.

181. ***The Company's Global Cybersecurity Strategist told the Company that its cybersecurity structure and practices were woefully insufficient.*** Shortly before the start of the Class Period, Ian Thornton-Trump, the Company's Global Cybersecurity Strategist, gave a presentation to several of the Company's top executives titled "Creating Security." Several of the Company's top executives—including Chief Technology Officer, Joe Kim; Chief Information

[60] *CRN*, "SolarWinds Execs Earned $65M In 2020 Despite Huge Hack," (Apr. 16, 2021), available at: https://www.crn.com/news/security/solarwinds-execs-earned-65m-in-2020-despite-huge-hack.

Officer, Rani Johnson; and Chief Marketing Officer, Gerardo Dada—attended the presentation. Both Mr. Kim and Mr. Dada reported directly to Defendant Thompson. During the presentation, Mr. Thornton-Trump told the executives that the Company's "infrastructure and corporate systems exist in a precarious state" and that, if the security deficiencies he identified at the Company were not addressed, the Company was putting itself at risk of a catastrophic cyberattack. *See* ¶¶74-80. He explicitly stated that "[t]he survival of the company depends on an internal commitment to security" and "[t]he survival of our customers depends on a commitment to build secure solutions." *See* ¶80.

182. Although the executives that attended Mr. Thornton-Trump's presentation agreed with his statements—which were often met with "a lot of nodding"—the Company did not implement the cybersecurity reforms. *See* ¶¶85-86; 90-102. Mr. Thornton-Trump was told the reason for the Company's refusal to reform: Defendant Thompson did not want to spend the money to implement the changes. *See* ¶¶85-86. Mr. Thornton-Trump resigned in protest, writing to a fellow executive that reported to Defendant Thompson that the Company was "unwilling to make the corrections necessary," causing him to "los[e] faith in the leadership" of the Company. His colleague, Chief Marketing Officer Gerardo Dada, "agree[d] with [his] assessment and ... appreciate[d] the effort and candor [he] put behind trying to do the right thing at SolarWinds."

183. That the Company's Global Cybersecurity Strategist told several of the Company's top executives that a failure to dramatically revamp the Company's seriously deficient cybersecurity practices would result in a catastrophic cyberattack supports the inference of scienter.

184. ***The Company failed to reform even <u>after</u> its Global Cybersecurity Strategist told the Company that its security structure and practices were woefully insufficient.*** As noted, after

Thornton-Trump delivered his Presentation, an attendee told him that "Kevin [Thompson] won't like spending th[e] kind of money" necessary to implement the reforms necessary to make the Company secure. *See* ¶85. That is precisely what happened: the Company did not reform its cybersecurity practices during the Class Period. Former employees of the Company recall that security trainings did not exist at SolarWinds (*see* ¶¶125-30), that employees could access parts of the Company's network that were unrelated to their job functions (*see* ¶¶131-36), that there was an absence of limitations on user access (*id.*), that no member of SolarWinds' senior leadership spoke about internal cybersecurity during the Class Period (*see* ¶¶142-45), that SolarWinds' employees were never instructed to change their passwords, and that there was no cybersecurity team at the Company (*see* ¶¶114-15). The Company's failure to reform its cybersecurity practices even after being specifically told by its Global Cybersecurity Strategist that its cybersecurity practices were insufficient strengthens the inference of scienter.

185. ***The Company knew that its Update Server had been compromised for one-and-a-half years.*** Since at least June of 2018, the Company's user credentials and password to its Update Server—"solarwinds123"—were publicly available on the website GitHub. *See* ¶¶105-07. Because they were publicly available, any person could access the Company's Update Server and insert malware into the updates that the Company sent to its customers. *Id.* The Company was told on November 19, 2019 that its Update Server had been compromised for over two years. *See* ¶¶109; 152. Recognizing the significance of the compromise, Defendant Brown and SolarWinds removed the password within an hour. *See* ¶112. Yet the Company did not disclose its cybersecurity deficiencies or fix them. SolarWinds' knowledge that the Company's password and user credentials to its critical Update Server were set by an intern and publicly available for a year-and-half further, and the haste with which the Company updated the Update Server's

password and credentials after being notified of the vulnerability, strengthens the inference scienter.

186. ***The Company repeatedly discussed the importance of cybersecurity, assuring investors that cybersecurity was a top priority for the Company.*** The Company detailed its purported commitment to cybersecurity in a formal Security Statement, which was featured prominently on the Company's website throughout the Class Period, and available through every page on the Company's website. *See* ¶¶35-42. Defendants also used their purported commitment to security to attempt to distinguish themselves from their competitors, repeatedly stressing that "strong vendors *publish* their security protocols and processes so you can evaluate whether they meet your standards," (*see* ¶39) assuring customers and investors that SolarWinds, unlike certain competitors, "places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards," (*see* ¶¶36; 39) and directing customers to its Security Center and Trust Center, where it assured customers and investors that the Company employed "[p]rocesses, procedures, and standards you can trust," explained that customers "security and privacy are our top priorities," and that the Company's "security strategy covers all aspects of [its] business." *See* ¶¶36-37. That the Company repeatedly spoke about cybersecurity best practices, touted the Company's ability to help customers implement cybersecurity best practices, and publicly stated its commitment to upholding cybersecurity best practices strengthens the scienter inference.

187. ***SolarWinds flagrantly violated its Security Statement.*** Despite repeatedly pointing to its Security Statement and assuring investors that cybersecurity was Defendants' top priority, SolarWinds flagrantly violated its own Security Statement for years and in virtually every respect. Numerous former employees of the Company have reported that the Company had no

security team (*see* ¶¶114-15); lacked a cybersecurity policy (*see* ¶¶116-18); lacked a password policy, with employees utilizing vulnerable passwords (*see* ¶¶119-24); failed to segment sensitive networks or assign user-roles to ensure that only employees that require access to the most sensitive data and networks can access them (*see* ¶¶131-36); failed to offer any cybersecurity training to its employees to ensure compliance with cybersecurity best practices (*see* ¶¶125-30); and failed to follow the NIST Cybersecurity Framework, including its requirement of employee background checks (*see* ¶¶137-39). That the Company violated its own Security Statement while repeatedly and publicly preaching the importance of each of these cybersecurity practices strengthens the inference of scienter.

188. ***Defendant Brown singled himself out as the SolarWinds executive responsible for security.*** Defendant Brown stated during the Class Period that he was "responsible for the security of [SolarWinds'] products ... as well as security for our infrastructure." *See* ¶16. Defendant Brown was also directly connected to the Company's Security Statement. Indeed, the Company's Security Center, which contained the Security Statement during a prior version of the Company's website during the Class Period, prominently featured a picture of Defendant Brown. *See* ¶38. Additionally, when investors or customers visited the "Security Center," they were met with a video introducing and featuring Defendant Brown, in which he stated that "I'm excited to share our new security resource center with everyone." *See id.* Having identified himself as intimately involved in the Company's "cybersecurity," Defendant Brown knew or, at minimum, was severely reckless in not knowing, of the Company's actual cybersecurity practices and absence of policies.

189. ***Cybersecurity was critical to the Company's customers.*** Cybersecurity was particularly important to SolarWinds' clients. The Company touted that its clients included all

five branches of the U.S. Military, the U.S. Pentagon, State Department, NASA, NSA, Postal Service, National Oceanic and Atmospheric Administration, Department of Justice, the Office of the President of the United States, the FBI, Secret Service, National Nuclear Security Administration, Veterans Affairs, and the Department of Homeland Security. *See* ¶34. Moreover, the Company's private sector clients included more than 425 of the U.S. Fortune 500 companies. *See id.* The nature of the Company's clients—government agencies whose data is necessarily sensitive and large private companies that necessarily are in possession of massive amounts of customer data—meant that cybersecurity was a particularly high priority for SolarWinds' clients.

190. ***The Company's failure to adopt cybersecurity practices allowed the Company to meet analyst consensus estimates.*** Defendant Thompson and SolarWinds' cost-cutting measures—and related failure to implement cybersecurity reforms—allowed the Company to report record profits during the Class Period. Had the Company devoted the necessary resources to cybersecurity—instead of engaging in cost-cutting measures intended to generate short-term profits—the Company would not have met analysts' estimates. Indeed, the Company has admitted that the necessary cybersecurity reforms will cost the Company $20 million to $25 million each year. Spending an additional $20 million to $25 million on cybersecurity in 2019—a year SolarWinds slightly exceeded analysts' net income expectations—would have caused the Company to miss consensus analyst estimates. For example, the Company exceeded consensus estimates for net income in the fourth quarter of 2018, and the first quarter of 2020, by less than $500,000, and by only $1.5 million in the second quarter of 2019—margins of less than 1% and 3%, respectively. Even in the fourth quarter of 2020, when the Company reported its highest revenue figure in the Class Period, the Company exceeded the consensus estimate for net income

by just over $2 million. That the Company's failure to implement cybersecurity reforms enabled it to meet analysts' expectations further strengthens the scienter inference.[61]

191. ***By misrepresenting their commitment to cybersecurity, Defendants were able to personally profit.*** Through their misrepresentations, Defendants were able to sell over $375 million in Company shares to investors as part of an initial public offering at the start of the Class Period. They were also able to conduct a follow-on offering of 15,000,000 shares at a price $3 higher than the IPO. All the shares sold in the follow-on offering were held by the Private Equity Firms—allowing them to net a total of over $260 million.

192. Additionally, through a multitude of Class Period sales, Defendant Thompson sold over one million shares of his personal SolarWinds common stock worth more than $20 million. Over the course of just three days in November 2020, Defendant Thompson sold 700,000 shares of his SolarWinds common stock—25% of his total beneficially-owned shares—netting him $15 million. This was the largest sale of SolarWinds stock in such a short period that Defendant Thompson ever conducted. By the end of the Class Period, Defendant Thompson had sold over one million shares, reflecting 39.16% of the shares he held at the beginning of the Class Period.

193. Defendant Thompson's stock sales during the Class Period were a significant departure from his prior trading pattern. Over an equivalent two-year and two-month length of time prior to the Class Period—from December 2013 until early February 2016, when the Private Equity Firms took SolarWinds private (the "Control Period")—Defendant Thompson sold just

[61] The Company's plans to spin off its MSP business, known as "N-able," was an additional incentive for the Company to increase revenue at all costs. As Defendant Thompson stated in an interview, the Company hoped to grow its spun-off MSP business at a rate significantly higher than is typical of SaaS businesses—generating 20 percent revenue growth or greater over a number of years, and up to 30 percent profit. *ChannelE2E*, "Kevin Thompson and John Pagliuca: The Interview," (Aug. 6, 2020), available at: https://www.channele2e.com/investors/thompson-pagliuca-potential-solarwinds-msp-spin-off/.

391,657 shares of the Company. Over 86% of these Control Period sales were "option-related," meaning that he exercised options and immediately sold the resulting shares—realizing no decrease in his total number of beneficially owned shares. Thus, during the Class Period, Defendant Thompson sold almost three times the amount of shares he sold during the Control Period. Excluding "option-related" sales, Defendant Thompson's Class Period sales are almost nineteen times greater than his Control Period sales.

194. Moreover, just one week before the revelation of the Company's cybersecurity deficiencies, the Private Equity Firms sold over $450 million of their SolarWinds stock. Had Defendants honestly represented to the public the state of SolarWinds' security practices, SolarWinds' common stock would have been trading significantly lower than the amounts that Defendant Thompson and the Private Equity Defendants sold their personal shares. By selling their shares prior to divulging the truth, Defendants Thompson and the Private Equity Firms profited millions of dollars. The amounts and suspicious timing of Defendants' stock sales further support the inference of scienter.

195. The timing of Defendants' stock sales is particularly suspicious in light of the fact that SolarWinds was notified in September 2020 by Palo Alto Networks, a California-based cybersecurity company, of the cybersecurity breach ultimately revealed to investors three months later—in December 2020. In September 2020, Palo Alto's Security Operation Center determined that a threat actor was attempting to infiltrate its network through SolarWinds' software. Palo Alto's Security Operations Center informed SolarWinds of the attempted breach and described the activity it observed on its network. That Defendant Thompson and the Private Equity Firms' largest stock sales took place within eight weeks of when they had received this information from

Palo Alto and shortly before news of the devastating hack was publicly disclosed further strengthens the scienter inference.

196. Not surprisingly, the SEC is conducting an ongoing investigation into Defendant Thompson and the Private Equity Firms' massive and suspiciously timed trades. As a former senior counsel in the SEC's Division of Enforcement put it, the timing of the Private Equity Firms' sales is "a formula for an insider trading investigation."[62]

197. Additionally, Defendant Thompson's compensation was tied to the Company's adjusted Earnings Before Interest, Taxes, Depreciation, and Amortization ("EBITDA"), giving him a motive to mislead investors as to SolarWinds' cybersecurity efforts and expenditures, while eschewing such expenditures in favor of short-term profits. Specifically, SolarWinds and its Board of Directors, a majority of which consisted of the Private Equity Firms' employees, tied Defendant Thompson's bonus—which was 135% of his base salary in 2018, and 125% of his base salary in 2019 and 2020—to the Company's revenue and adjusted EBITDA performance metrics.[63]

198. ***The Company has admitted its cybersecurity practices were deficient.*** After the Class Period, the Company announced its "Secure by Design" initiative, which is comprised of a host of cybersecurity reforms intended to shore up its cybersecurity practices. *See* ¶¶168-75. The Company outlined changes to its password management, limited access privileges, and network segmentation policies and practices—all areas of cybersecurity that the Company claimed to have

---

[62] *The Washington Post*, "Investors in breached software firm SolarWinds traded $280 million in stock days before hack was revealed," (Dec. 15, 2020), available at: https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/.

[63] The Company defined adjusted EBITDA in its SEC filings as "net income or loss, excluding the impact of purchase accounting on total revenue, amortization of acquired intangible assets and developed technology, depreciation expense, stock-based compensation expense and related employer-paid payroll taxes, restructuring and other charges, acquisition and Sponsor related costs, interest expense, net, debt extinguishment and refinancing costs, unrealized foreign currency (gains) losses, and income tax expense (benefit)."

implemented during the Class Period. *See id.* The Company admitted that the Company's need to reform was significant, and would necessitate tens-of-millions of dollars in expenses and the hiring of additional personnel. That the Company belatedly implemented a host of cybersecurity practices that it claimed to follow during the Class Period further contributes to the strong inference of scienter.

199. The foregoing facts, particularly when considered collectively (as they must be), support a strong inference of Defendants' scienter.

VI. DEFENDANTS' MATERIALLY FALSE AND MISLEADING STATEMENTS AND OMISSIONS

200. Defendants made numerous materially false and misleading statements and omissions concerning the Company's cybersecurity during the Class Period, as detailed further below.

A. Defendants' Materially False and Misleading Statements and Omissions in Their "Security Statement"

201. Throughout the Class Period, the Company maintained, and prominently featured on its website, a document titled the SolarWinds "Security Statement." The Security Statement contained a series of representations about SolarWinds' purported cybersecurity practices. These representations were false and misleading.

202. ***The "Security Team."*** In the Security Statement, SolarWinds represented that the Company had a "security team [that] focuses on information security, global security auditing and compliance, as well as defining the security controls for protection of SolarWinds' hardware infrastructure." SolarWinds further stated that "[i]nformation security roles and responsibilities are defined within the organization" and represented that the "security team receives information system security notifications on a regular basis and distributes security alert and advisory

information to the organization on a routine basis after assessing the risk and impact as appropriate."

203. The Company's statements set forth above in ¶202 above were false, misleading, and omitted material facts. Numerous SolarWinds employees have explained that the Company lacked both a security team and defined security roles, and failed to focus on security within the organization. *See* ¶¶114-15; 140-49. Security was not even discussed within the Company, and short-term growth and cost-cutting were management's lone priorities. *See* ¶¶142-49.

204. ***The "Information Security Policy."*** In the Security Statement, SolarWinds also stated that the Company "maintains a written Information Security Policy." The Company's "Information Security Policy" purportedly "cover[ed] a wide array of security related topics ranging from general standards with which every employee must comply, such as account, data, and physical security, to more specialized security standards covering internal applications and information systems." SolarWinds represented that it "receive[d] signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before providing authorized access to SolarWinds information systems."

205. The Company's statements in ¶204 above were false and misleading. SolarWinds employees have explained that the Company did not have an Information Security Policy, and employees were never asked to sign any Information Security Policy. *See* ¶¶116-18. Security was not even discussed within the Company, and short-term growth and cost-cutting were management's lone priorities. *See* ¶¶142-49.

206. ***Security Training.*** In the Security Statement, the Company stated that "[e]mployees are provided with security training as part of new hire orientation" and that "each

SolarWinds employee is required to read, understand, and take a training course on the company's code of conduct."

207. The Company's statements in ¶206 above were false and misleading. SolarWinds employees have reported that the Company did not provide cybersecurity training to its employees, and that they were not required to undergo cybersecurity training at any time during their employment. *See* ¶¶125-30.

208. ***The "Password Policy."*** In the Security Statement, the Company represented that it and its employees adhered to a strict password policy. The Company stated that "[o]ur password policy covers all applicable information systems, applications, and databases," with SolarWinds employing "password best practices [that] enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords." It further represented that its "[p]asswords are individually salted and hashed."

209. The Company's statements in ¶208 above were false and misleading. As SolarWinds employees have explained, the Company did not have a password policy; employees never received any direction or training as to secure passwords; the Company and its employees used vulnerable, non-unique passwords that were not "individually salted and hashed" (e.g., "solarwinds123"), including for critical servers; critical passwords were "hard-coded" and not changed; and critical passwords, including to access the Update Server, were publicly available. *See* ¶¶119-24.

210. ***Limiting User Authorization and Segmenting Networks.*** SolarWinds further represented to investors in its Security Statement that the Company restricted which Company employees could access its various databases. In a section of is Security Statement titled "Authentication and Authorization," the Company stated that SolarWinds employees are only

"granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet" and beyond that, employees are only "granted access to certain additional resources based on their specific job function." The Company further assured investors and customers that it applied "Role Based Access controls," explaining that "[r]ole based access controls are implemented for access to information systems" and that "[a]ccess controls to sensitive data in [Company] databases, systems, and environments are set on a need-to-know / least privilege necessary basis." SolarWinds further emphasized that "[b]y default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need."

211. Further, SolarWinds represented in its Security Statement that SolarWinds "maintains separate development and production environments," with "adequate network segmentation through the establishment of security zones that control the flow of network traffic."

212. The Company's statements in ¶¶210-11 above were false and misleading. Contrary to Defendants' representations, the Company did not limit user authorization or segment networks. *See* ¶¶131-36. As multiple SolarWinds employees have explained, Company employees had access to servers within the organization outside their roles and were permitted to access servers and customer accounts that they should not have had authorization to access. *See id.*

213. ***Adherence to the NIST Cybersecurity Framework.*** SolarWinds bolstered the specific representations in its Security Statement with the further assurance that the Company "follows the NIST [National Institute of Standards and Technology] Cybersecurity Framework."

214. The NIST's Cybersecurity Framework requires that "[a]ccess to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions." It further requires that "[t]he organization's personnel and partners are provided

cybersecurity awareness education and are adequately trained to perform their information and security-related duties and responsibilities consistent with related policies, procedures, and agreements." It further mandates that "[t]he organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information and security-related duties and responsibilities consistent with related policies, procedures, and agreements." It additionally requires that companies "[d]o a full, nationwide criminal background check … on all prospective employees."

215. The Company's statement in ¶213 was false and misleading. The Company did not adhere to the NIST Cybersecurity Framework. As numerous SolarWinds employees have explained, SolarWinds did not limit user authorization and segment networks (*see* ¶¶131-36); SolarWinds did not provide cybersecurity training to its employees (*see* ¶¶125-30); and SolarWinds did not perform background checks on prospective employees (*see* ¶¶137-39).

B. Defendants' Additional Materially False and Misleading Statements and Omissions on the SolarWinds Website

216. Throughout the Class Period, the Company maintained a page on its website entitled "Security at SolarWinds," which could be accessed from anywhere on the website by selecting "Security Information" from a banner on each page. At the top of the Security at SolarWinds page, the Company stated:

> SolarWinds is committed to taking our customers security and privacy concerns seriously and makes it a priority. We strive to implement and maintain security processes, procedures, standards, and take all reasonable care to prevent unauthorized access to our customer data. We apply appropriate administrative, operational, and technical security controls to help ensure that our customer data is handled and processed in a responsible and secure manner.

217. The Company's statements in ¶216 above were false and misleading and omitted material facts. The Company did not "make [security] a priority" or apply appropriate security controls. As set forth above, the Company maintained deficient cybersecurity practices in order

to cut costs. *See* ¶¶140-49. Defendants' statements in ¶216 were also false and misleading because they omitted material facts about the Company's cybersecurity deficiencies, including that the Company (i) did not have a password policy (*see* ¶¶119-24); (ii) failed to implement a password policy despite employees utilizing vulnerable passwords (*see id.*), (iii) failed to segment sensitive networks or assign user-roles to ensure that only employees that require access to the most sensitive data and networks can access them (*see* ¶¶131-36), (iv) failed to offer any cybersecurity training to its employees to ensure compliance with cybersecurity best practices (*see* ¶¶125-30), (v) lacked a cybersecurity policy (*see* ¶¶116-18), (vi) lacked a security team (*see* ¶¶114-15), and (vii) failed to follow the NIST Cybersecurity Framework, including its requirement of employee background checks (*see* ¶¶137-39).

218. During the Class Period, the Company also maintained a page on its website entitled the "SolarWinds Trust Center," which could be accessed from anywhere on the website by selecting "Trust Center" from a banner on each page. Near the top of the SolarWinds Trust Center, the Company stated, "[y]our security and privacy are our top priorities at SolarWinds."

219. The Company's statement in ¶218 above was materially false and misleading when made and omitted material facts. The Company did not "make [security] a priority" or "apply appropriate ... security controls." As set forth above, the Company maintained deficient cybersecurity practices in order to cut costs. *See* ¶¶142-49. Defendants' statements in ¶218 were also false and misleading because they omitted material facts about the Company's cybersecurity deficiencies, including that the Company (i) did not have a password policy (*see* ¶¶119-24); (ii) failed to implement a password policy, with employees utilizing vulnerable passwords (*see id.*), (iii) failed to segment sensitive networks or assign user-roles to ensure that only employees that require access to the most sensitive data and networks can access them (*see* ¶¶131-36), (iv) failed

to offer any cybersecurity training to its employees to ensure compliance with cybersecurity best practices (*see* ¶¶125-30), (v) lacked a cybersecurity policy (*see* ¶¶116-18), (vi) lacked a security team (*see* ¶¶114-15), and (vii) failed to follow the NIST Cybersecurity Framework, including its requirement of employee background checks (*see* ¶¶137-39).

C. Defendants' Additional Materially False and Misleading Statements and Omissions Throughout the Class Period

1. March 14, 2019 Interview

220. On March 14, 2019, Defendant Brown appeared on the SolarWinds Techpod podcast, which is maintained on its website. During the interview, Defendant Brown emphasized the Company's purported commitment to security, stating:

> SolarWinds has, I think, 56 countries and huge environments. So one of the things that we've focused on, that my team focuses on, is on heavy-duty hygiene, right? We look at every log, we understand when somebody logs in, we understand when somebody is trying to gain access to an administrative account, we understand which systems have updated antivirus on them. We do that every day and it is one of the hardest and unsexiest parts of security that there is. It really is, but it's what is so important to do well.

221. Defendant Brown's statement in ¶220 above was false and misleading and omitted material facts. SolarWinds did not focus on "heavy-duty hygiene." As SolarWinds employees have observed, the Company's actual focus was growing the SolarWinds business—not cybersecurity. *See* ¶¶140-49. Defendants' statements in ¶220 were also false and misleading because they omitted material facts about the Company's cybersecurity deficiencies, including that the Company (i) did not have a password policy (*see* ¶¶119-24); (ii) failed to implement a password policy, with employees utilizing vulnerable passwords (*see id.*), (iii) failed to segment sensitive networks or assign user-roles to ensure that only employees that require access to the most sensitive data and networks can access them (*see* ¶¶131-36), (iv) failed to offer any cybersecurity training to its employees to ensure compliance with cybersecurity best practices (*see* ¶¶125-30),

(v) lacked a cybersecurity policy (*see* ¶¶116-18), (vi) lacked a security team (*see* ¶¶114-15), and (vii) failed to follow the NIST Cybersecurity Framework, including its requirement of employee background checks (*see* ¶¶137-39).

2. April 30, 2019 Interview

222. On April 30, 2019, in an article published on the Company's website, Defendant Brown was interviewed by Aviva Zacks. Zacks asked Defendant Brown, "[h]ow is SolarWinds preparing to stay ahead of the curve?" In his answer, Defendant Brown stated, "[W]e're working on a lot of different things including putting identity solutions in place. We are making sure that there is good basic hygiene...."

223. Defendant Brown's statement in ¶222 above was materially false and misleading when made and omitted material facts. The Company did not "mak[e] sure that there [was] good basic hygiene." As set forth above, the Company maintained deficient cybersecurity practices in order to cut costs. *See* ¶¶140-49. Defendants' statement in ¶222 was also false and misleading because they omitted material facts about the Company's cybersecurity deficiencies, including that the Company (i) did not have a password policy (*see* ¶¶119-24); (ii) failed to implement a password policy, with employees utilizing vulnerable passwords (*see id.*), (iii) failed to segment sensitive networks or assign user-roles to ensure that only employees that require access to the most sensitive data and networks can access them (*see* ¶¶131-36), (iv) failed to offer any cybersecurity training to its employees to ensure compliance with cybersecurity best practices (*see* ¶¶125-30), (v) lacked a cybersecurity policy (*see* ¶¶116-18), (vi) lacked a security team (*see* ¶¶114-15), and (vii) failed to follow the NIST Cybersecurity Framework, including its requirement of employee background checks (*see* ¶¶137-39).

VII. LOSS CAUSATION

224. Defendants' misstatements and omissions concerning the Company's commitment to security and adherence to the representations in its Security Statement artificially inflated the price of SolarWinds' stock. The artificial inflation in SolarWinds' stock price was removed when the conditions and risks misstated and omitted by Defendants and/or the materialization of the risks concealed by Defendants' material misstatements and omissions were revealed to the market. These disclosures and/or materializations divulged or revealed information through a series of partial disclosing events, which slowly corrected Defendants' prior misrepresentations and omissions and/or revealed facts about the nature and extent of SolarWinds' security deficiencies. These disclosures and/or materializations of the risk, more particularly described below, reduced the amount of artificial inflation in the price of SolarWinds' publicly traded stock, causing economic injury to Lead Plaintiff and other members of the Class.

225. On December 13, 2020, a Sunday, *Reuters* reported that hackers had infiltrated the U.S. Treasury and Commerce Departments and had been monitoring email accounts within both departments. *Reuters* reported that a SolarWinds product was believed to be the source of the hack. SolarWinds itself then confirmed the breach, stating that cybercriminals gained access to SolarWinds' Update Server and inserted malicious computer code, called "malware," that SolarWinds distributed to clients in the form of routine software updates. Also on December 13, 2020, CISA released an emergency directive directing all federal civilian agencies to immediately disconnect from their networks all SolarWinds' Orion products. The CISA emergency directive—one of only five such emergency directives issued since 2015—tied the emergency measure

directly to the Company's deficient cybersecurity practices, stating that the vulnerability in the SolarWinds product "poses unacceptable risks to the security of federal networks."

226. On December 14, 2020, SolarWinds filed a Form 8-K formally disclosing the hack to shareholders, announcing that the cybercriminals "inserted a vulnerability within its Orion monitoring products which … could potentially allow an attacker to compromise the server on which the Orion products run." SolarWinds further revealed that the breach occurred between March and June 2020, and that the number of customers believed to have installed the malware numbered as many as 18,000. Reporting began to reveal the massive scope of the attack. *The New York Times* reported that the federal agencies that had been infiltrated included the Department of Homeland Security and the Department of Defense. The reporting further noted that "[n]early all Fortune 500 companies … use SolarWinds products" as does "Los Alamos National Laboratory, where nuclear weapons are designed." *Politico* quoted a U.S. official with knowledge of the attack as saying, "'This is probably going to be one of the most consequential cyberattacks in U.S. history…. That's the view from inside government – that we're dealing with something of a scale that I don't think we've had to deal with before.'"

227. SolarWinds' stock tumbled 17% in direct response to these revelations, from $23.55 on the close of the prior trading day to $19.62 on December 14, 2020 on heavy trading volume. Analysts were shocked at the disclosure of the breach and immediately tied the precipitous stock drop to the shocking announcement to the breach. Barclays wrote, "This morning, SolarWinds put out a press release acknowledging that its Orion software platform was targeted in potentially broad-reaching cyberattacks …. We highlight that Orion suite is the integrated SolarWinds platform across its core IT products … [which] made up 45% of its total revenue ytd across all customers …. Overall, we believe shares will remain under pressure as

investors worry about potential financial and legal impacts to the company and as the events continue to unfold." Jefferies concurred, writing, "Key Takeaway: SWI was down 17% after it announced a security compromise that impacts the Orion NM product. The bad news is that the fed govt., a major vertical, has frozen the software and that this event will have an impact on revs. and new deals …."

228. However, the full scope of Defendants' woeful security measures and the breach were not fully known. As a CISA official told *Politico*, "'Many agencies don't know how on fire they are yet,'" with another government official agreeing that "'[w]e are in very, very early days, and there's a sense that … the news is going to get worse.'"

229. On December 15, 2020, *The Wall Street Journal* reported that the list of federal agencies known to have been compromised "grew substantially," now including the "National Institutes of Health and the State Department." It was also revealed that "[n]ational security agencies and defense contractors … were among those breached …."

230. Reporting on the Company's security practices also began to emerge, further coloring investors' perceptions of the Company and contextualizing the breach as part of the Company's deficient cybersecurity practices. *Reuters* reported that the Company was previously warned that the password to access the internal server to the Update Server, "solarwinds123," was both incomprehensibly deficient from a security perspective and also publicly available on the internet. *Reuters* further reported that, despite the growing realization of the significance of the breach, the Company left the malware that was the source of the attack available for download on its Update Server for several days.

231. On December 15, 2020, SolarWinds' stock fell 8% in direct response to the further revelations regarding the attack, from $19.62 on December 14, 2020 to $18.06 on December 15,

2020 on heavy trading volume, with shocked analysts tying the drop directly to the continuing revelations. For instance, RBC Capital Markets wrote that, "[w]hile the situation is fluid, our view is that the cyber attack introduces an incremental reputational risk to the story and around fourth quarter new business and renewal opportunities. As such, we believe shares are likely to remain under pressure in the near-term...." RBC Capital Markets lowered its price estimate on SolarWinds' stock "as we will look to gather additional details" on the attack.

232. On December 17, 2020, further details of the Company's deficient cybersecurity and resultant breach emerged. Microsoft President Brad Smith revealed that more than 40 of its customers were victims of the attack. Five large information technology companies, including Deloitte, also announced they were breached as a result of SolarWinds' products. *Bloomberg* reported that at least three state governments were also compromised, and the cybercriminals had also infiltrated the Department of Energy and the National Nuclear Security Administration—the source of the United States' nuclear codes.

233. SolarWinds' stock plummeted a further 19% in direct response to the further revelations, from $17.60 on December 17, 2020 to $14.18 on December 18, 2020 on heavy trading volume, with analysts tying the stock's freefall directly to the continuing news about the Company's central role in the historic attack. Wedbush wrote in a December 18, 2020 report: "To put it bluntly, based on all the initial data and speaking with our Beltway contacts last night/today we believe this cyber-attack will likely rank as one of the worst (very possibly the worst ever) in the last decade given the targeted and cyber espionage nature of this attack." Jefferies, in a December 21, 2020 report, concurred: "SWI has lost 40% of its value or ~3B over the past wk .... [W]e believe this is the worst hack for a software company .... The hack will in all likelihood have an impact on results next year."

234. It was foreseeable that Defendants' materially false and misleading statements and omissions discussed herein would artificially inflate the price of SolarWinds securities and that the ultimate disclosure of the information detailed herein, or the materialization of the risks concealed by Defendants' material misstatements and omissions, would cause the price of SolarWinds' securities to decline. The decline in SolarWinds' stock price was a direct and proximate result of the truth being revealed to investors and to the market.

VIII. INAPPLICABILITY OF THE STATUTORY SAFE HARBOR

235. The statutory safe harbor applicable to forward-looking statements under certain circumstances does not apply to any of the false or misleading statements pleaded in this Complaint. The statements complained of herein were historical statements or statements of current facts and conditions at the time the statements were made. Further, to the extent that any of the false or misleading statements alleged herein could be construed as forward-looking, the statements were not accompanied by any meaningful cautionary language identifying important facts that could cause actual results to differ materially from those in the statements.

236. Alternatively, to the extent the statutory safe harbor otherwise would apply to any forward-looking statements pleaded herein, Defendants are liable for those false and misleading forward-looking statements because at the time each of those statements was made, the speakers knew the statement was false or misleading, or the statement was authorized or approved by an executive officer of SolarWinds who knew that the statement was materially false or misleading when made.

237. Additionally, the risk disclosures included in SolarWinds' public filings were inadequate, obfuscated the truth, and did not inform investors of the true facts and actual risks already occurring.

IX. PRESUMPTION OF RELIANCE

238. Lead Plaintiff is entitled to a presumption of reliance on Defendants' material misrepresentations and omissions pursuant to the fraud-on-the-market doctrine because, during the Class Period:

a. SolarWinds' common stock was actively traded in an efficient market on the NYSE;

b. SolarWinds' common stock traded at high weekly volumes;

c. As a regulated issuer, SolarWinds filed periodic public reports with the SEC;

d. SolarWinds regularly communicated with public investors by means of established market communication mechanisms, including through regular dissemination of press releases and through other wide-ranging public disclosures, such as communications with the financial press, securities analysts and other similar reporting services;

e. The market reacted promptly to public information disseminated by SolarWinds;

f. SolarWinds securities were covered by numerous securities analysts employed by major brokerage firms who wrote reports that were distributed to the sales force and certain customers of their respective firms. Each of these reports was publicly available and entered the public marketplace;

g. The material misrepresentations and omissions alleged herein would tend to induce a reasonable investor to misjudge the value of SolarWinds securities; and

h. Without knowledge of the misrepresented or omitted material facts alleged herein, Lead Plaintiff and other members of the Class purchased or acquired SolarWinds common stock between the time Defendants misrepresented or omitted material facts and the time the true facts were disclosed.

239. Lead Plaintiff is also entitled to a presumption of reliance under *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972), because the claims asserted herein against Defendants are predicated upon omission of material fact that there was a duty to disclose.

240. Accordingly, Lead Plaintiff and other members of the Class relied, and are entitled to have relied, upon the integrity of the market prices for SolarWinds' common stock, and are entitled to a presumption of reliance on Defendants' materially false and misleading statements and omissions during the Class Period.

X. CLASS ACTION ALLEGATIONS

241. Lead Plaintiff brings this action as a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of a Class consisting of all persons and entities who purchased or otherwise acquired securities issued by SolarWinds during the period from October 18, 2018 to December 17, 2020, inclusive, and who were damaged thereby. Excluded from the Class are Defendants; SolarWinds' affiliates and subsidiaries; the officers and directors of SolarWinds and its subsidiaries and affiliates at all relevant times; members of the immediate family of any excluded person; heirs, successors, and assigns of any excluded person or entity; and any entity in which any excluded person has or had a controlling interest.

242. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, SolarWinds common shares were actively traded on the New York Stock Exchange. As of October 2020, there were over 314 million shares of SolarWinds common stock outstanding. Although the exact number of Class members is unknown to Lead Plaintiff at this time, Lead Plaintiff believes that there are at least thousands of members of the proposed Class. Members of the Class can be identified from records maintained by SolarWinds or its transfer agent(s), and may be notified of the pendency of this action by publication using a form of notice similar to that customarily used in securities class actions.

243. Lead Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class were similarly damaged by Defendants' conduct as complained of herein. Common questions of law and fact exist to all members of the Class and predominate over any

questions solely affecting individual members of the Class. Among the questions of fact and law common to the Class are:

a. whether Defendants' misrepresentations and omissions as alleged herein violated the federal securities laws;

b. whether the Control Person Defendants are personally liable for the alleged misrepresentations and omissions described herein;

c. whether Defendants' misrepresentations and omissions as alleged herein caused the Class members to suffer a compensable loss; and

d. whether the members of the Class have sustained damages, and the proper measure of damages.

244. Lead Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class actions and securities litigation. Lead Plaintiff has no interest that conflicts with the interests of the Class.

245. A class action is superior to all other available methods for the fair and efficient adjudication of this action. Joinder of all Class members is impracticable. Additionally, the damages suffered by some individual Class members may be small relative to the burden and expense of individual litigation, making it practically impossible for such members to redress individually the wrongs done to them. There will be no difficulty in the management of this action as a class action.

XI. CLAIMS FOR RELIEF

COUNT I
VIOLATIONS OF SECTION 10(B) OF THE EXCHANGE ACT AND RULE 10b-5 PROMULGATED THEREUNDER
(Against SolarWinds and the Executive Defendants)

246. Lead Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

247. This Count is asserted on behalf of all members of the Class against all Defendants for violations of Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b) and Rule 10b-5 promulgated thereunder, 17 C.F.R. § 240.10b-5.

248. During the Class Period, Defendants disseminated, furnished information for inclusion in, or approved the false statements specified above, which they knew were, or they deliberately disregarded as, misleading in that they contained misrepresentations and omitted material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

249. During the Class Period, Defendants carried out a plan, scheme, and course of conduct which was intended to and, throughout the Class Period, did: (i) deceive the investing public, including Lead Plaintiff and other Class members, as alleged herein; and (ii) cause Lead Plaintiff and other members of the Class to purchase SolarWinds common stock at artificially inflated prices.

250. Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 in that they: (i) employed devices, schemes, and artifices to defraud; (ii) made untrue statements of material fact and/or omitted to state material facts necessary to make the statements not misleading; and (iii) engaged in acts, practices, and a course of business which operated as a fraud and deceit upon the purchasers of the Company's common stock in an effort to maintain artificially high market prices for SolarWinds common stock.

251. Defendants, individually and in concert, directly and indirectly, by the use, means or instrumentalities of interstate commerce and/or of the mails, engaged and participated in a continuous course of conduct that operated as a fraud and deceit upon Lead Plaintiff and the Class; made various untrue and/or misleading statements of material facts and omitted to state material

facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; made the above statements intentionally or with severe recklessness; and employed devices and artifices to defraud in connection with the purchase and sale of SolarWinds common stock, which were intended to, and did: (a) deceive the investing public, including Lead Plaintiff and the Class, regarding, among other things, SolarWinds' cybersecurity practices; (b) artificially inflate and maintain the market price of SolarWinds common stock; and (c) cause Lead Plaintiff and other members of the Class to purchase SolarWinds common stock at artificially inflated prices and suffer losses when the true facts became known and/or the risks materialized.

252. Defendants are liable for all materially false and misleading statements made during the Class Period, as alleged above.

253. As described above, Defendants acted with scienter throughout the Class Period, in that they acted either with intent to deceive, manipulate, or defraud, or with severe recklessness. The misrepresentations and omissions of material facts set forth herein, which presented a danger of misleading buyers or sellers of SolarWinds stock, were either known to the Defendants or were so obvious that the Defendants should have been aware of them.

254. Lead Plaintiff and the Class have suffered damages in that, in direct reliance on the integrity of the market, they paid artificially inflated prices for SolarWinds' common stock, which inflation was removed from its price when the true facts became known.

255. Defendants' wrongful conduct, as alleged above, directly and proximately caused the damages suffered by Lead Plaintiff and other Class members. Had Defendants disclosed complete, accurate, and truthful information concerning these matters during the Class Period, Lead Plaintiff and other Class members would not have purchased or otherwise acquired

SolarWinds securities or would not have purchased or otherwise acquired these securities at the artificially inflated prices that they paid. It was also foreseeable to Defendants that misrepresenting and concealing these material facts from the public would artificially inflate the price of SolarWinds' securities and that the ultimate disclosure of this information, or the materialization of the risks concealed by Defendants' material misstatements and omissions, would cause the price of SolarWinds securities to decline.

256. Accordingly, as a result of their purchases of SolarWinds common stock during the Class Period, Lead Plaintiff and the Class suffered economic loss and damages under the federal securities laws.

257. By virtue of the foregoing, Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5, promulgated thereunder.

258. This claim is brought within the applicable statute of limitations.

COUNT II
VIOLATIONS OF SECTION 20(A) OF THE EXCHANGE ACT
(Against the Control Person Defendants)

259. Lead Plaintiff repeats, incorporates, and reallege each and every allegation set forth above as if fully set forth herein.

260. As alleged above, SolarWinds and the Executive Defendants each violated Section 10(b) and Rule 10b-5 thereunder by their acts and omissions as alleged in this Complaint.

261. This count is asserted on behalf of all members of the Class against the Control Person Defendants for violations of Section 20(a) of the Exchange Act, 15 U.S.C. § 78t(a).

262. At all relevant times, the Control Person Defendants were controlling persons of the Company within the meaning of Section 20 of the Exchange Act.

263. By virtue of the Executive Defendants' high-level positions, participation in and/or awareness of the Company's operations, direct involvement in the day-to-day operations of the

Company, and/or intimate knowledge of the Company's actual performance, and their power to control the materially false and misleading public statements about SolarWinds during the Class Period, the Executive Defendants had the power and ability to control the actions of SolarWinds and its employees.

264. The Controlling Entity Defendants exercised control over the Company through their financing of the Company, significant share ownership of the Company during the Class Period and having their own senior executives, and executives over which they exercise control, on the Company's Board of Directors during the Class Period.

265. SolarWinds identified itself as a "controlled company" in its SEC filings during the Class Period. The Private Equity Firms owned over 80% of SolarWinds' stock at the start of the Class Period and exercised control over SolarWinds throughout the Class Period. SolarWinds admitted to investors in its Annual Report filed on Form 10-K that, because of their large share of the voting power of the Company, the Private Equity Firms "could exert significant influence over [SolarWinds'] operations and business strategy and would together have sufficient voting power to effectively control the outcome of matters requiring stockholder approval."

266. The Company also noted in its public disclosures that the Private Equity Firms had the right to designate a majority of SolarWinds' Board of Directors, and those designated directors were entitled to constitute majorities of all committees other than the audit committee. Finally, the Company disclosed that this "concentration of ownership of [SolarWinds] common stock could delay or prevent proxy contests, mergers, tender offers, open-market purchase programs or other purchases of our common stock that might otherwise give [investors] the opportunity to realize a premium over the then-prevailing market price of our common stock."

267. The Controlling Entity Defendants were also controlling persons of their agents on the Company's Board of Directors because they were the employers of these individuals and controlled the manner in which these individuals voted as directors. Specifically:

a. James Lines was an Operating Partner, and then a Senior Operating Partner, at Thoma Bravo and a member of the SolarWinds Board at the same time throughout the Class Period.

b. Jason White was a Director of Silver Lake and a member of the SolarWinds Board since February 2016 and through February 2020.

c. Mike Widmann was a Director of Silver Lake and a member of the SolarWinds Board since February 2020 and throughout the remainder of the Class Period.

d. Seth Boro was a Managing Partner at Thoma Bravo and a member of the SolarWinds Board at the same time throughout the Class Period.

e. Kenneth Y. Hao was a Chairman and Managing Partner at Silver Lake and a member of the SolarWinds Board at the same time throughout the Class Period.

f. Mike Bingle was a Managing Partner and Managing Director at Silver Lake and a member of the SolarWinds Board at the same time throughout the Class Period.

g. Michael Hoffmann was a Principal at Thoma Bravo and a member of the SolarWinds Board at the same time throughout the Class Period.

268. The Controlling Entity Defendants had the power and ability to control the actions of SolarWinds and its employees, including by virtue of Lines, Widmann, Boro, Hao, Bingle and Hoffman's membership on the SolarWinds Board, participation in and awareness of the Company's operations, direct involvement in the day-to-day operations of the Company, and intimate knowledge of the Company's actual performance, their ability to gain access to all SolarWinds reports, agendas and other information available to members of the SolarWinds board

of directors, and their power to control the materially false and misleading public statements about SolarWinds during the Class Period.

269. By reason of the aforementioned conduct, the Control Person Defendants are liable under Section 20 of the Exchange Act jointly and severally with and to the same extent as SolarWinds and the Executive Defendants are liable under Section 10 of the Exchange Act to Lead Plaintiff and all members of the Class.

XII. PRAYER FOR RELIEF

WHEREFORE, Lead Plaintiff prays for judgment against Defendants as follows:

A. Declaring that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure;

B. Awarding compensatory damages in favor of Lead Plaintiff and other Class members against all Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Awarding Lead Plaintiff and the Class their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

D. Awarding such equitable/injunctive or other further relief as the Court may deem just and proper.

XIII. JURY DEMAND

270. Lead Plaintiff demands a trial by jury.

DATED: June 1, 2021

MARTIN & DROUGHT, P.C.

Gerald T. Drought
State Bar No. 06134800
Federal Bar No. 8942
Frank B. Burney
State Bar No. 03438100
Weston Centre
112 E. Pecan Street, Suite 1616
San Antonio, Texas 78205
Tel: (210) 227-7591
Fax: (210) 227-7924
gdrought@mdtlaw.com

Liaison Counsel for Lead Plaintiff New York City District Council of Carpenters Pension Fund

BERNSTEIN LITOWITZ BERGER & GROSSMANN LLP

John J. Rizio-Hamilton (admitted *pro hac vice*)
Jonathan D. Uslaner (admitted *pro hac vice*)
Benjamin W. Horowitz (admitted *pro hac vice*)
Thomas Z. Sperber (admitted *pro hac vice*)
1251 Avenue of the Americas
New York, New York 10020
Telephone: (212) 554-1400
Facsimile: (212) 554-1444
Johnr@blbglaw.com
JonathanU@blbglaw.com
Benjamin.Horowitz@blbglaw.com
Thomas.Sperber@blbglaw.com

Lead Counsel for Lead Plaintiff New York City District Council of Carpenters Pension Fund and the Class